EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale and importation of the Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,873,595 (the "'595 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '595 Patent by providing its customers and others with the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

10,873,595 Claim 1	Evidence
1. A method, comprising: at at least one server: identifying first vulnerability information utilizing second vulnerability information that is used to identify a plurality of potential vulnerabilities, the first vulnerability information being identified by:	ManageEngine, when in operation, practices a method comprising: *a server* (Vulnerability Manager Plus Server) *and identifying first vulnerability information utilizing second vulnerability information* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and is generated using information available on a Central Vulnerability Database) *that is used to identify a plurality of potential vulnerabilities* (e.g., a Vulnerability Manager Plus then scans your network for software/zero-day vulnerabilities and displays them in a dedicated view in the console) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

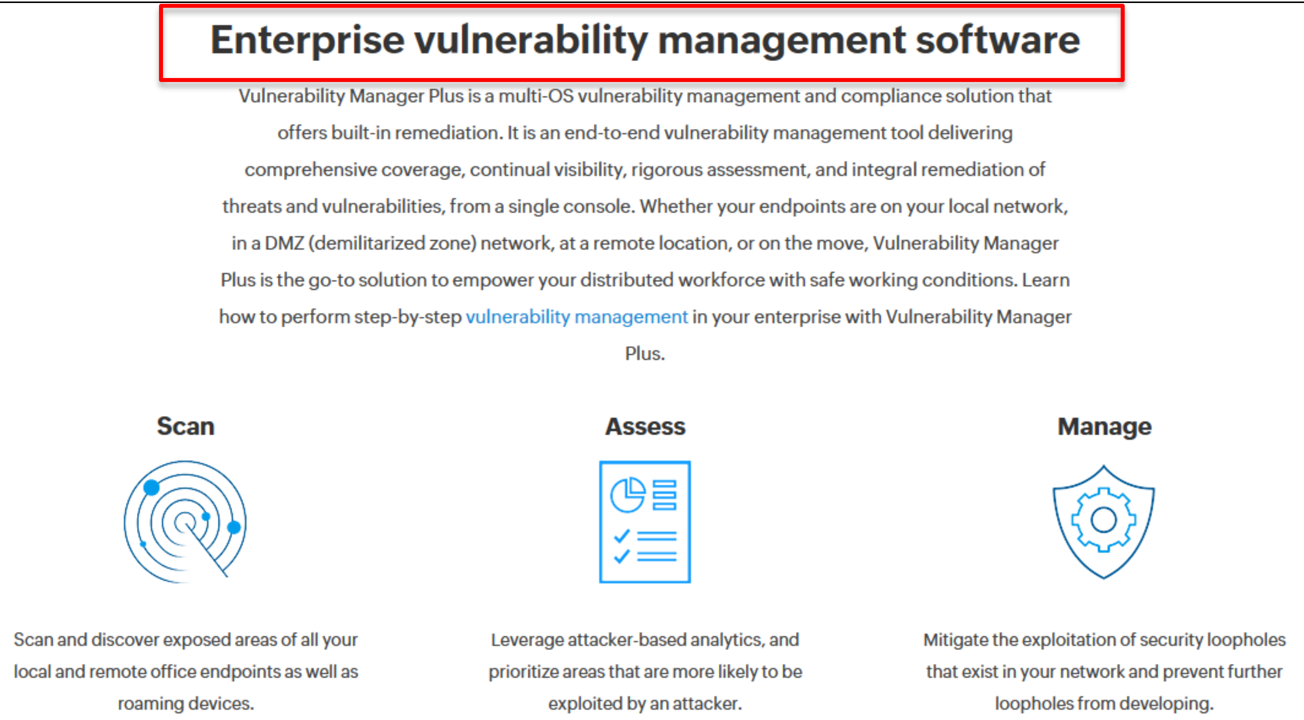
	 **Enterprise vulnerability management software** Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager Plus. **Scan** Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices. **Assess** Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker. **Manage** Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing. https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

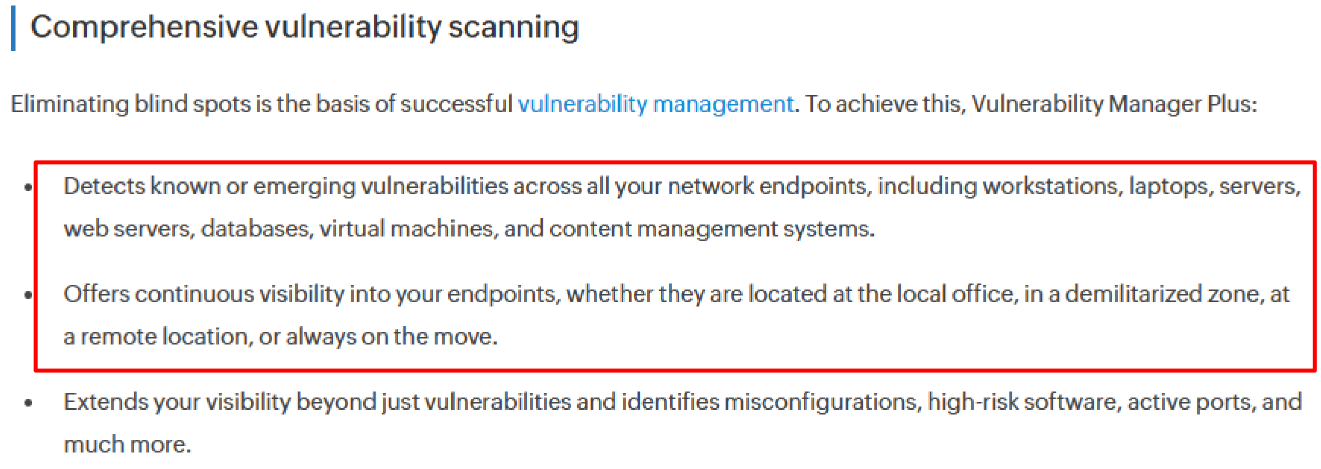
	 Comprehensive vulnerability scanning Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus: • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

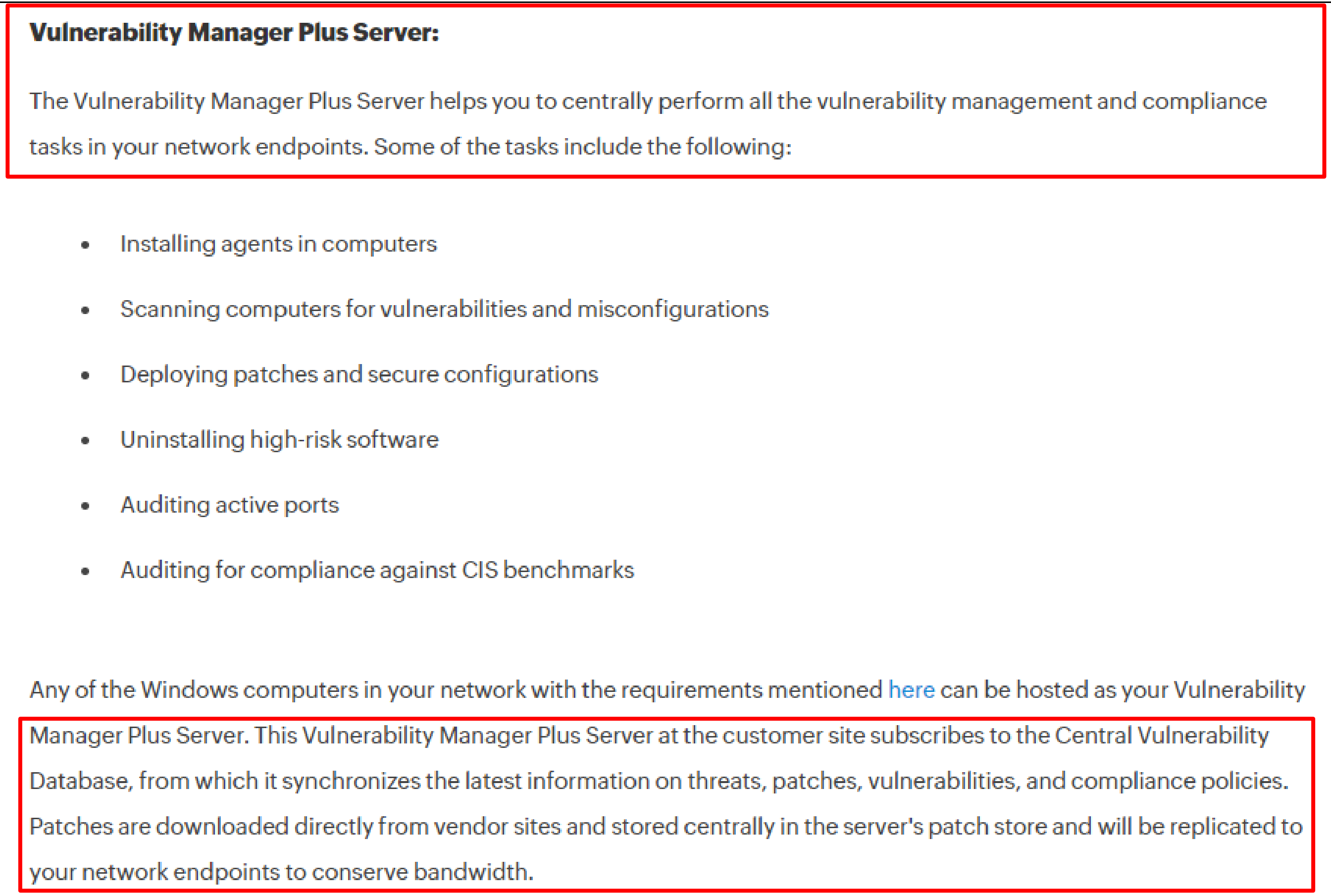
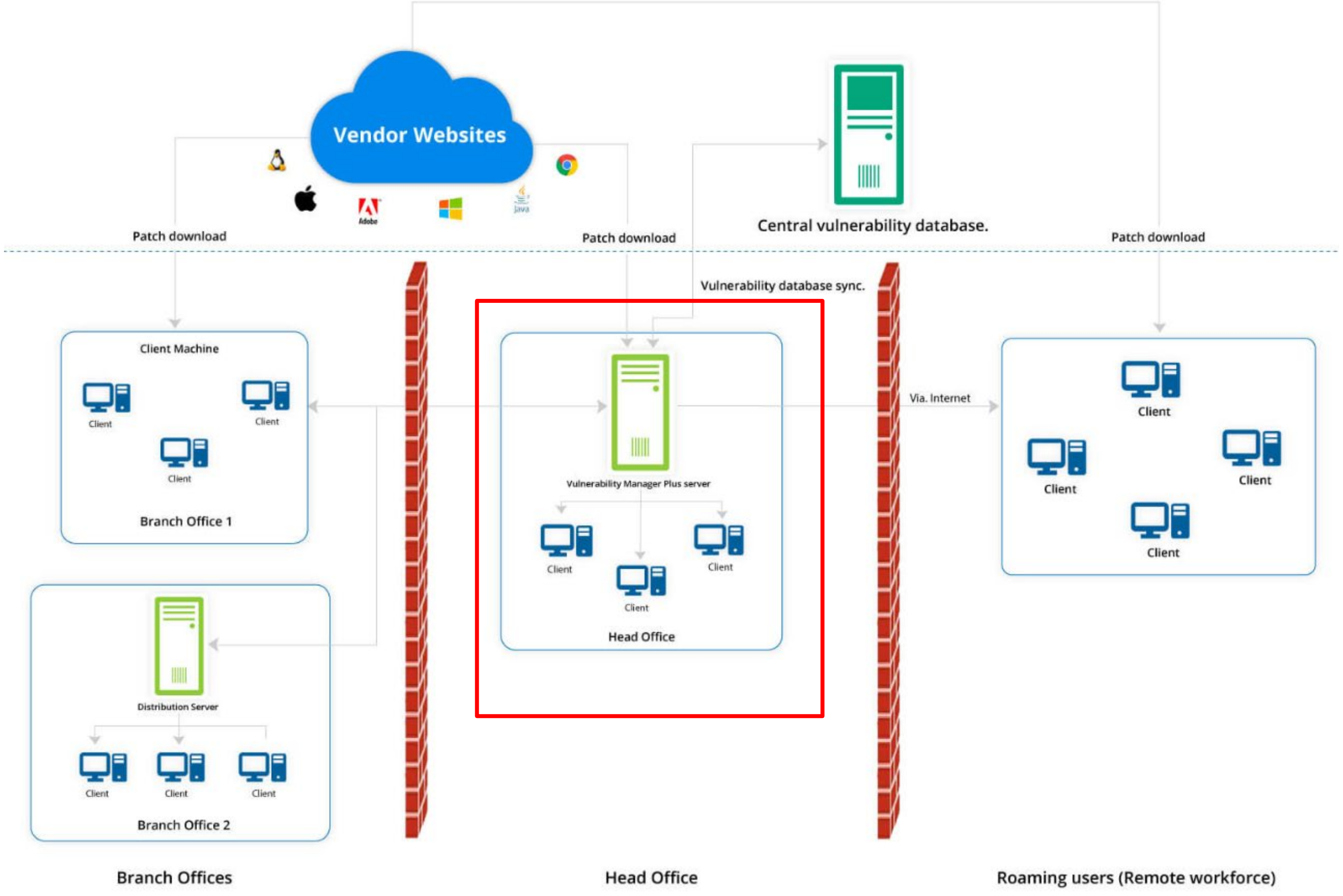
	 **Vulnerability Manager Plus Server:** The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following: • Installing agents in computers • Scanning computers for vulnerabilities and misconfigurations • Deploying patches and secure configurations • Uninstalling high-risk software • Auditing active ports • Auditing for compliance against CIS benchmarks Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth. https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1

EXHIBIT 10

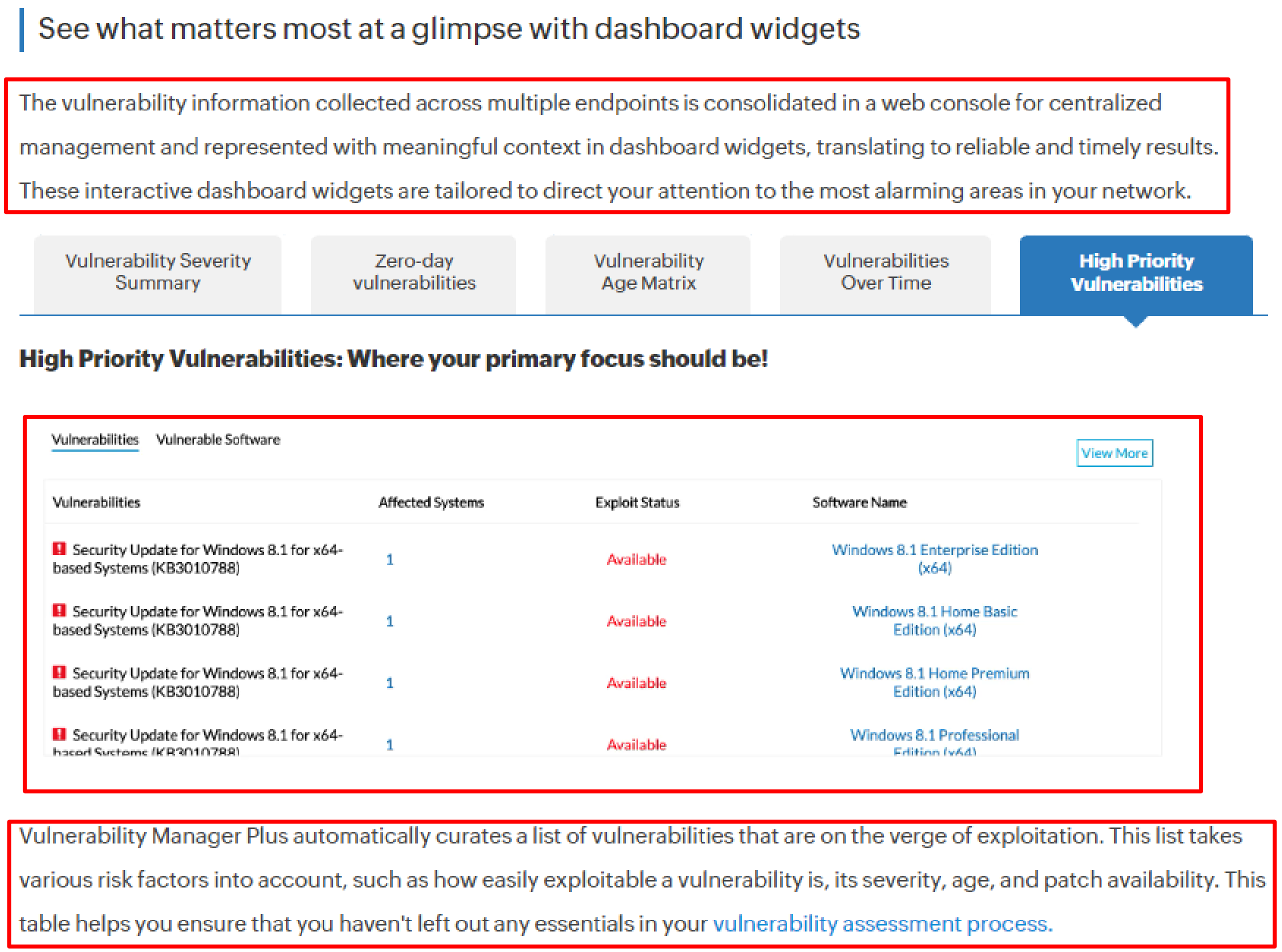
U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td></td>
<td>


https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg
</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity Summary
Zero-day vulnerabilities
Vulnerability Age Matrix
Vulnerabilities Over Time
High Priority Vulnerabilities

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities	Affected Systems	Exploit Status	Software Name
❗ Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
❗ Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
❗ Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
❗ Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.

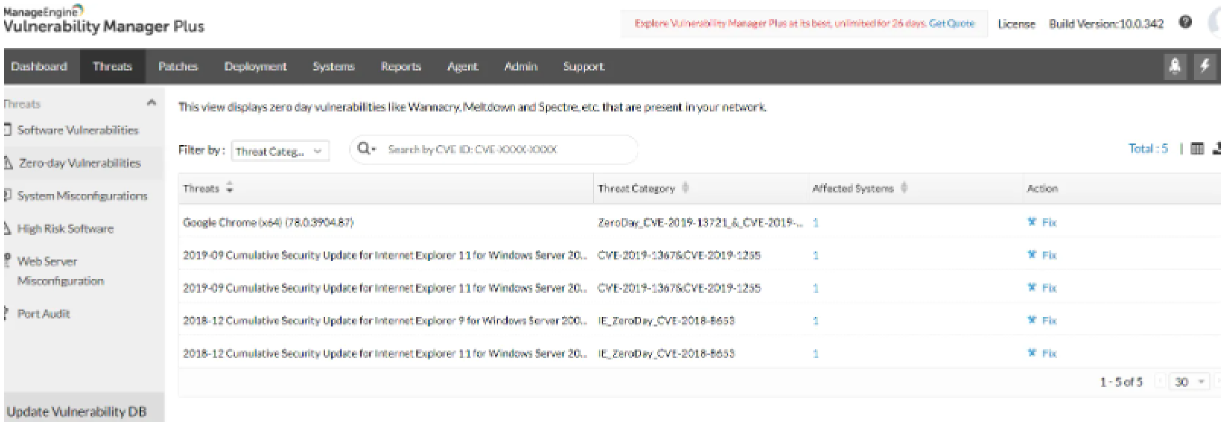
https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.

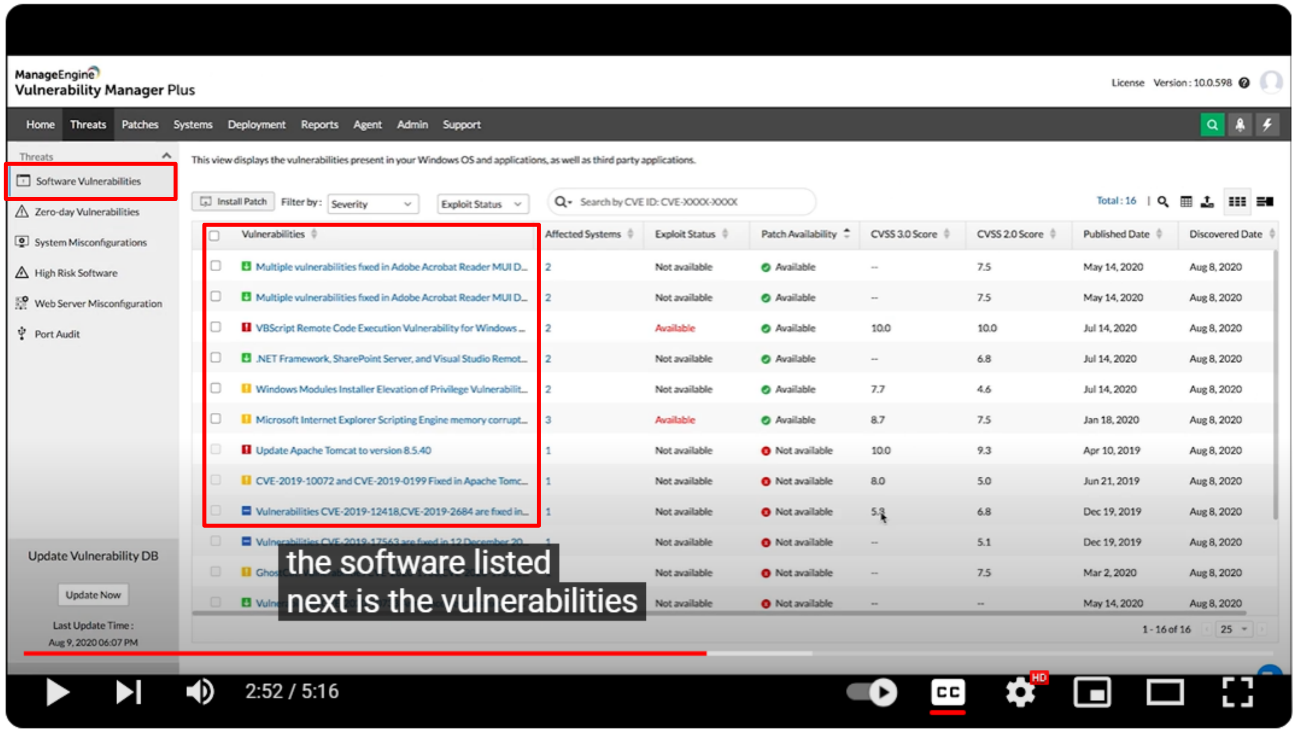
Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



ManageEngine Vulnerability Manager Plus

Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
Ghos[illegible]	[illegible]	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vulne[illegible]	[illegible]	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

the software listed
next is the vulnerabilities

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

identifying at least one operating system of a plurality of devices, and based on the at least one operating system, identifying	ManageEngine, when in operation, practices a method for *identifying at least one operating system of a plurality of devices* (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., on Windows or Mac endpoints, etc.) *and identifying at least one of the plurality of potential vulnerabilities as an actual vulnerability of a plurality of actual vulnerabilities of the at least one operating system to which the plurality of devices is actually vulnerable* (e.g., OS vulnerabilities are determined and under the software

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

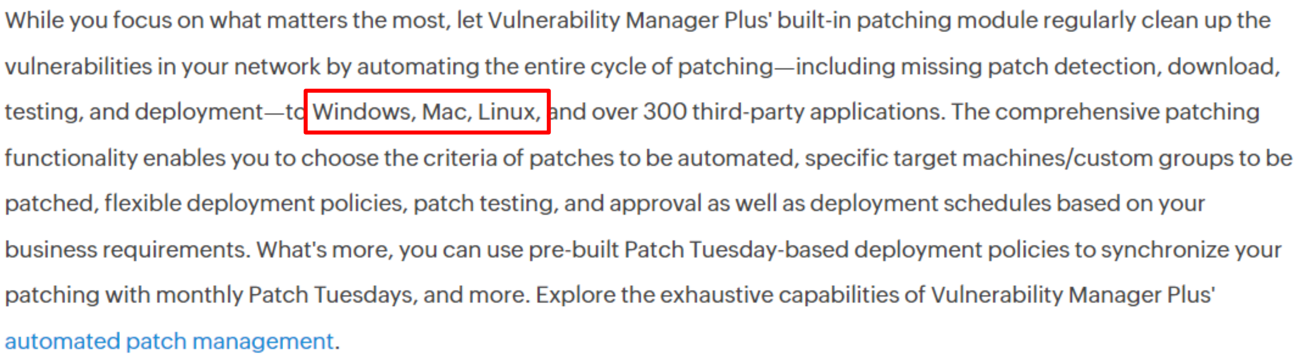
at least one of the plurality of potential vulnerabilities as an actual vulnerability of a plurality of actual vulnerabilities of the at least one operating system to which the plurality of devices is actually vulnerable; and	vulnerabilities section list of all potential vulnerabilities are displayed along corresponding number of the affected systems) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  While you focus on what matters the most, let Vulnerability Manager Plus' built-in patching module regularly clean up the vulnerabilities in your network by automating the entire cycle of patching—including missing patch detection, download, testing, and deployment—to Windows, Mac, Linux, and over 300 third-party applications. The comprehensive patching functionality enables you to choose the criteria of patches to be automated, specific target machines/custom groups to be patched, flexible deployment policies, patch testing, and approval as well as deployment schedules based on your business requirements. What's more, you can use pre-built Patch Tuesday-based deployment policies to synchronize your patching with monthly Patch Tuesdays, and more. Explore the exhaustive capabilities of Vulnerability Manager Plus' automated patch management. https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

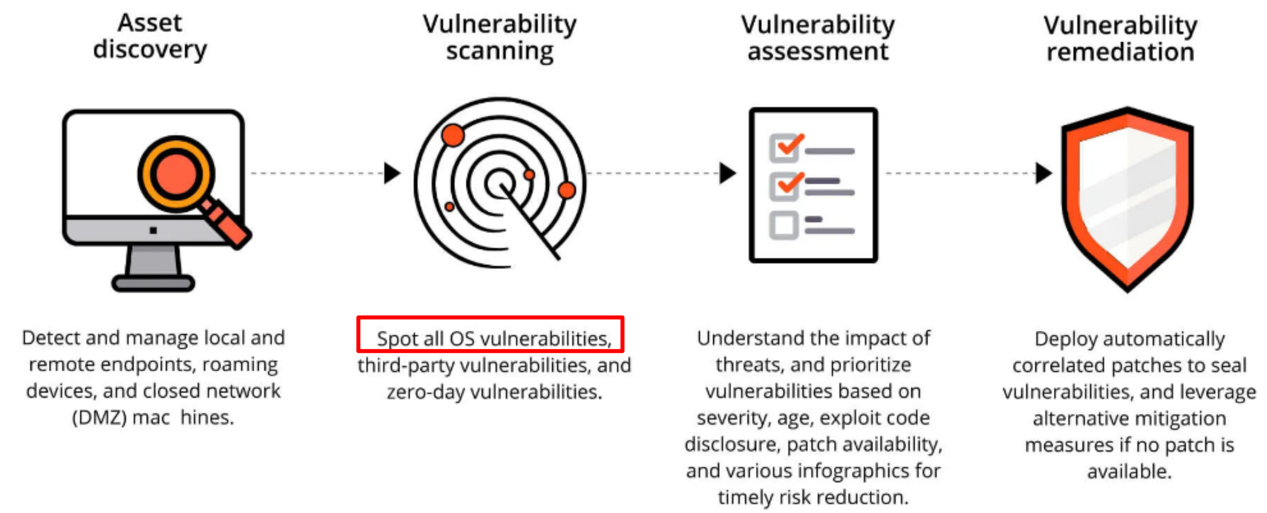
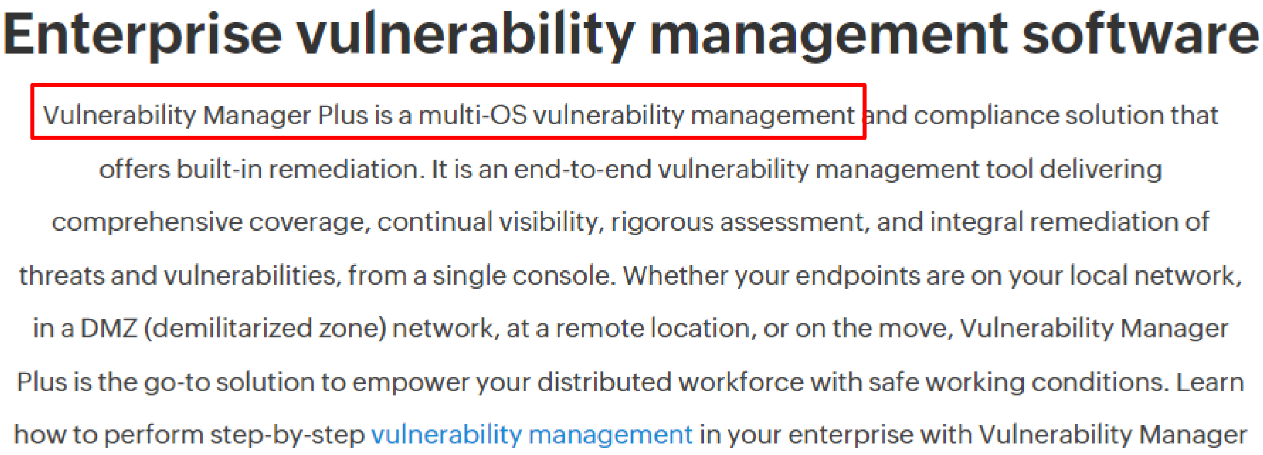
	 Asset discovery Vulnerability scanning Vulnerability assessment Vulnerability remediation Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) mac hines. Spot all OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities. Understand the impact of threats, and prioritize vulnerabilities based on severity, age, exploit code disclosure, patch availability, and various infographics for timely risk reduction. Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available. https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html  **Enterprise vulnerability management software** Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

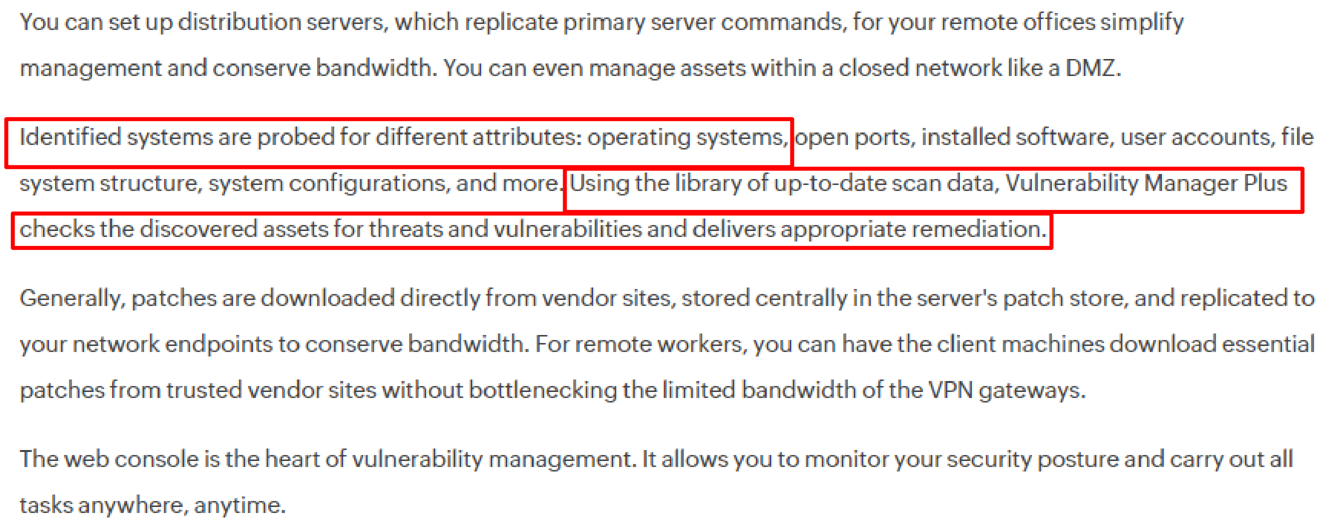
	https://www.managengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS  You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ. Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation. Generally, patches are downloaded directly from vendor sites, stored centrally in the server's patch store, and replicated to your network endpoints to conserve bandwidth. For remote workers, you can have the client machines download essential patches from trusted vendor sites without bottlenecking the limited bandwidth of the VPN gateways. The web console is the heart of vulnerability management. It allows you to monitor your security posture and carry out all tasks anywhere, anytime. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

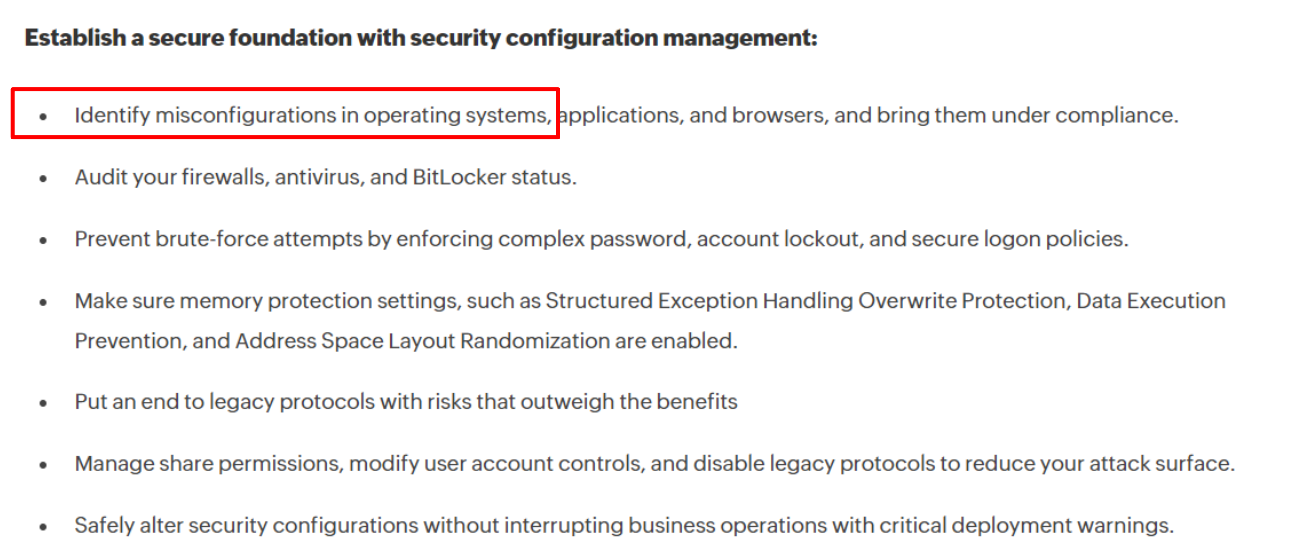
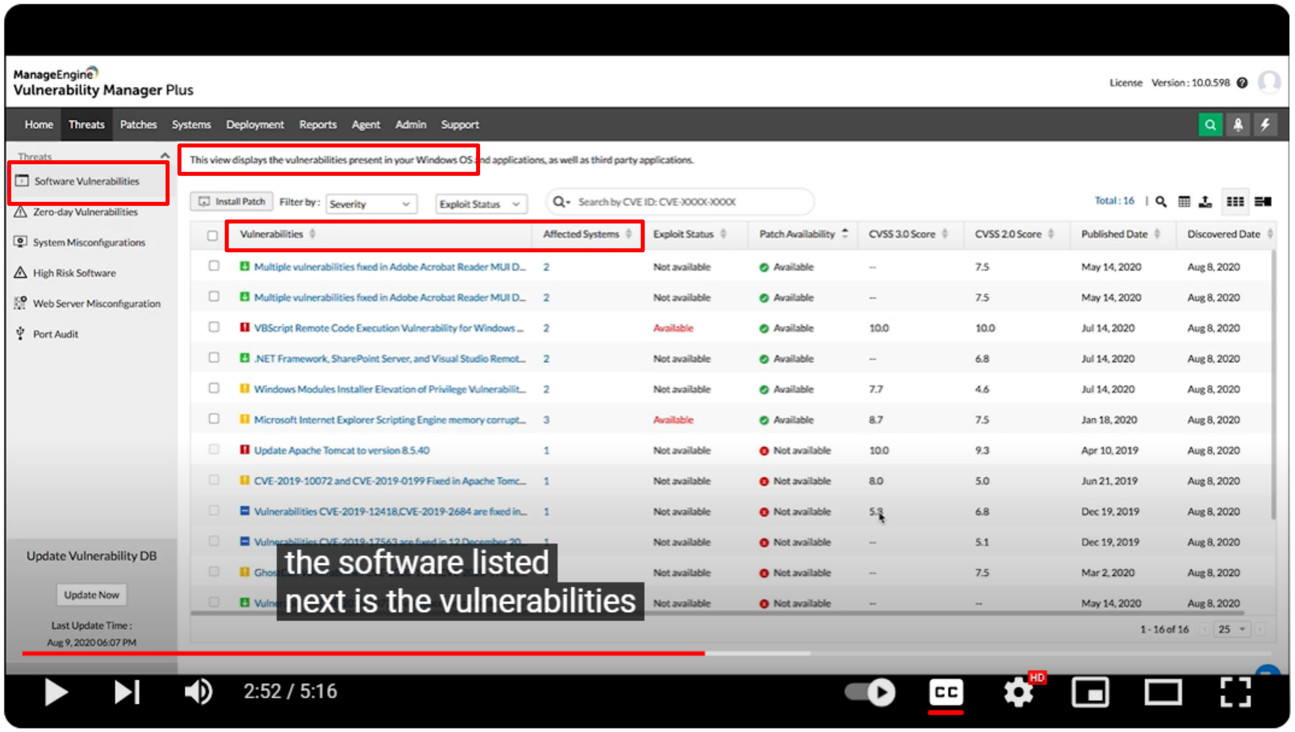
	 **Establish a secure foundation with security configuration management:** • Identify misconfigurations in operating systems, applications, and browsers, and bring them under compliance. • Audit your firewalls, antivirus, and BitLocker status. • Prevent brute-force attempts by enforcing complex password, account lockout, and secure logon policies. • Make sure memory protection settings, such as Structured Exception Handling Overwrite Protection, Data Execution Prevention, and Address Space Layout Randomization are enabled. • Put an end to legacy protocols with risks that outweigh the benefits • Manage share permissions, modify user account controls, and disable legacy protocols to reduce your attack surface. • Safely alter security configurations without interrupting business operations with critical deployment warnings. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.3	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
Ghos[illegible]	[illegible]	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vuln[illegible]	[illegible]	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

the software listed
next is the vulnerabilities

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

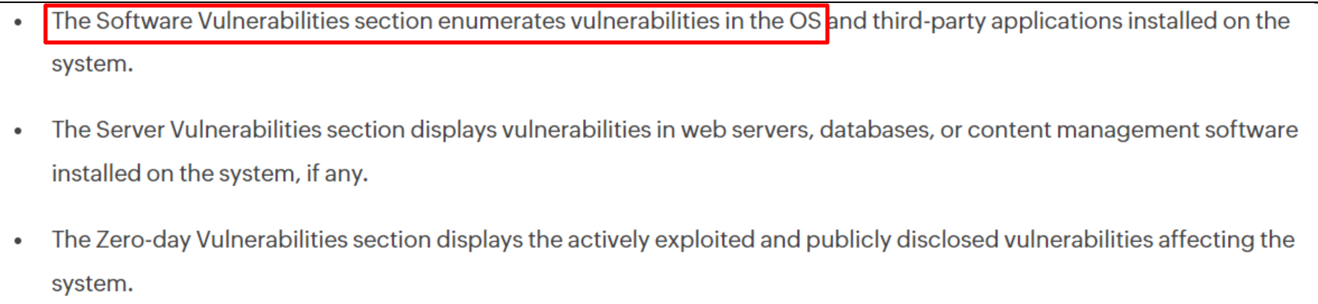
	 • The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system. • The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any. • The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system. https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html
communicating, from the at least one server and to at least one of the plurality of devices over at least one network, the first vulnerability information, the first vulnerability information corresponding with the actual vulnerabilities of the at least one operating system of the at least one device, and excluding at least a portion of the second vulnerability	ManageEngine, when in operation, practices a method for *communicating, from the at least one server and to at least one of the plurality of devices over at least one network, the first vulnerability information,* (e.g., Vulnerability Manager Plus Server provides the vulnerability information to various endpoints or clients over network) *the first vulnerability information corresponding with the actual vulnerabilities of the at least one operating system of the at least one device,* (e.g., OS vulnerabilities are determined and under the software vulnerabilities section that provides list of all potential vulnerabilities which are displayed along corresponding number of the affected systems) *and excluding at least a portion of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., a custom group is created as per the operating system wherein a vulnerability or misconfiguration is excluded for a specific custom group) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

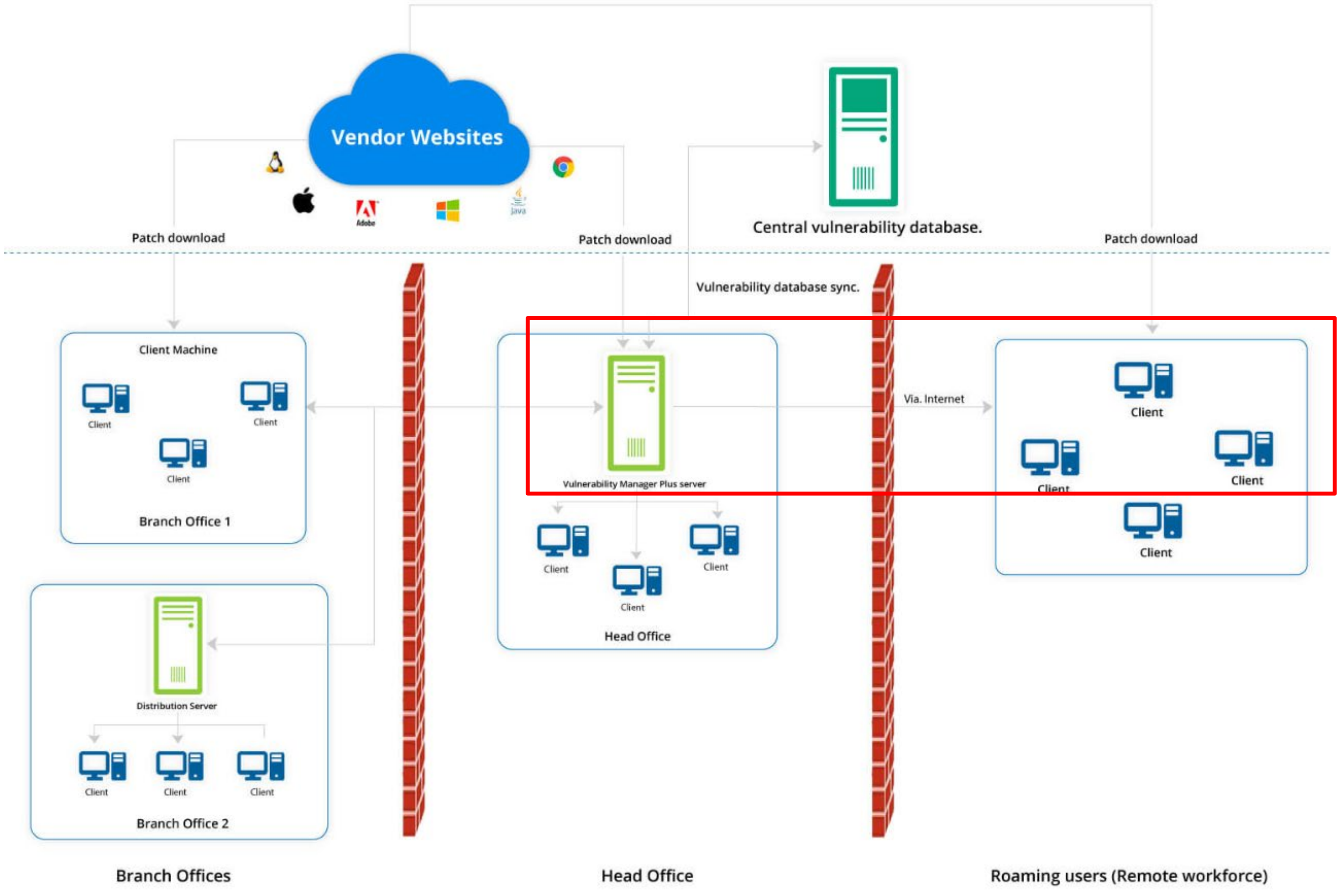
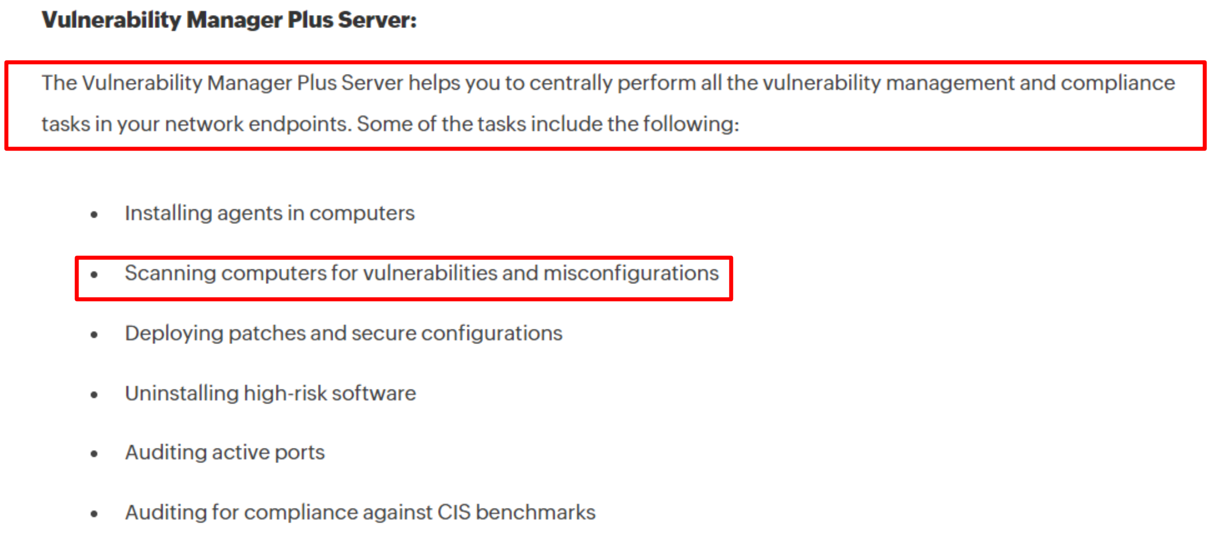
information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	 Vendor Websites Adobe Java Central vulnerability database. Patch download Patch download Patch download Vulnerability database sync. Client Machine Client Client Client Branch Office 1 Vulnerability Manager Plus server Client Client Client Head Office Via. Internet Client Client Client Client Distribution Server Client Client Client Branch Office 2 Branch Offices Head Office Roaming users (Remote workforce) https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

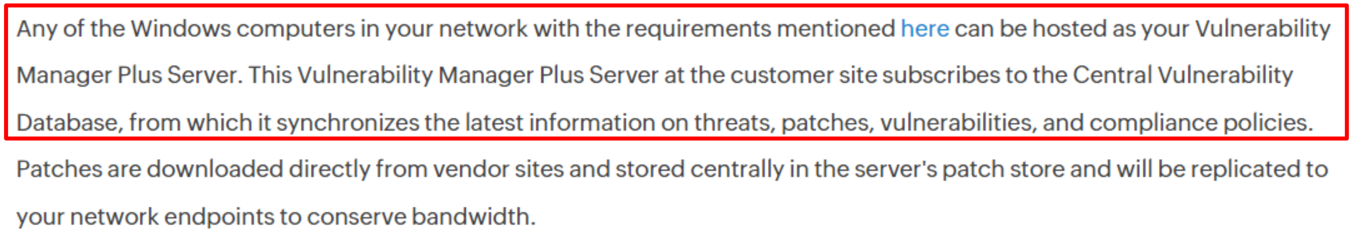


Vulnerability Manager Plus Server:

The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:

- Installing agents in computers
- Scanning computers for vulnerabilities and misconfigurations
- Deploying patches and secure configurations
- Uninstalling high-risk software
- Auditing active ports
- Auditing for compliance against CIS benchmarks

https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html



Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

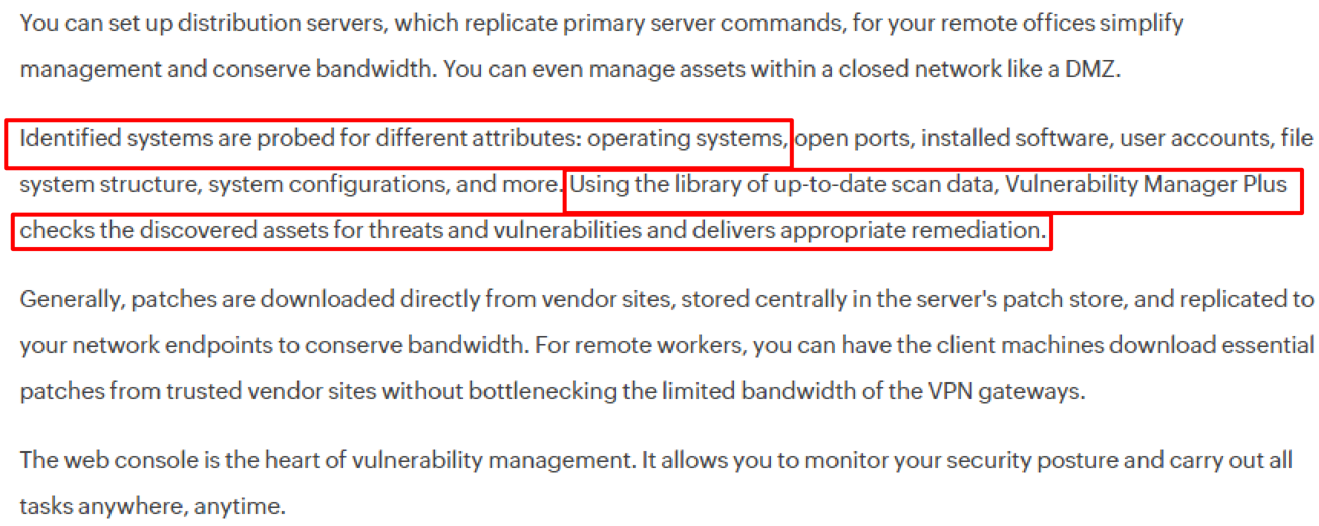
	 You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ. Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation. Generally, patches are downloaded directly from vendor sites, stored centrally in the server's patch store, and replicated to your network endpoints to conserve bandwidth. For remote workers, you can have the client machines download essential patches from trusted vendor sites without bottlenecking the limited bandwidth of the VPN gateways. The web console is the heart of vulnerability management. It allows you to monitor your security posture and carry out all tasks anywhere, anytime. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

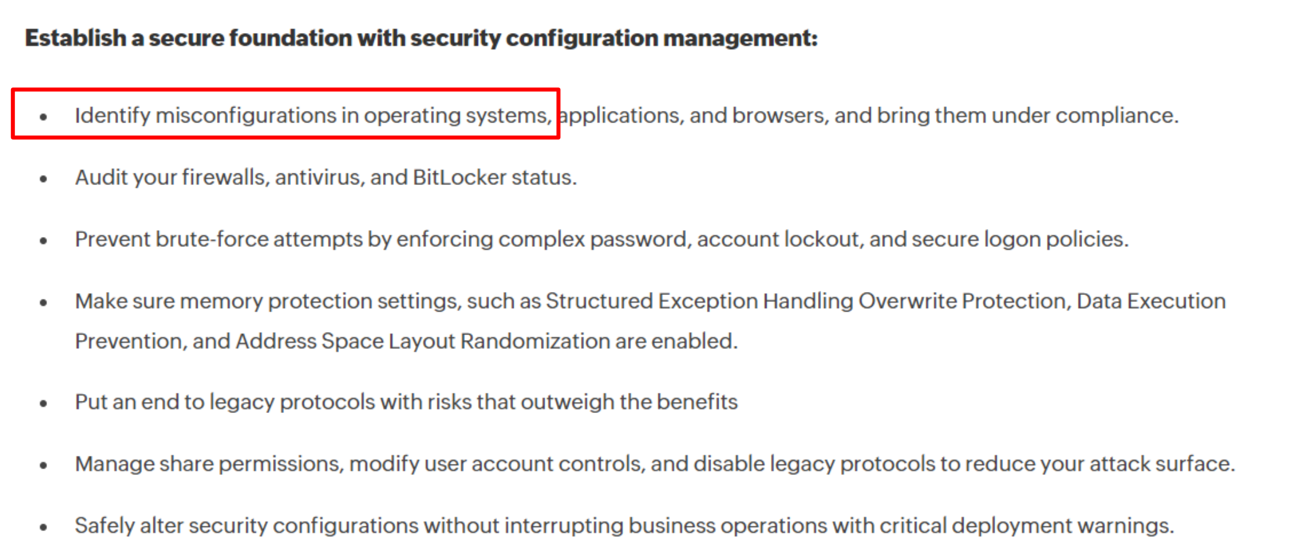
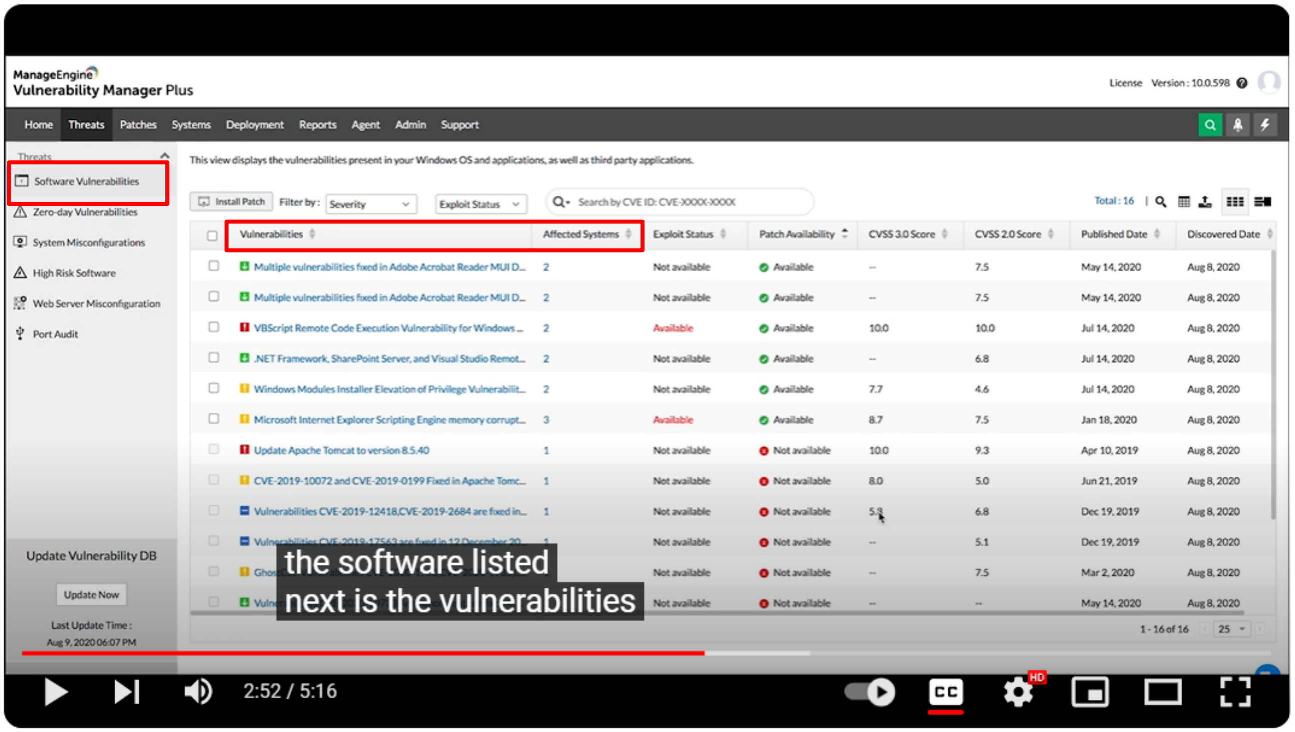
	 **Establish a secure foundation with security configuration management:** • Identify misconfigurations in operating systems, applications, and browsers, and bring them under compliance. • Audit your firewalls, antivirus, and BitLocker status. • Prevent brute-force attempts by enforcing complex password, account lockout, and secure logon policies. • Make sure memory protection settings, such as Structured Exception Handling Overwrite Protection, Data Execution Prevention, and Address Space Layout Randomization are enabled. • Put an end to legacy protocols with risks that outweigh the benefits • Manage share permissions, modify user account controls, and disable legacy protocols to reduce your attack surface. • Safely alter security configurations without interrupting business operations with critical deployment warnings. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Filter by : Severity | Exploit Status | Search by CVE ID: CVE-XXXX-XXXX

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
Ghos [illegible]	[illegible]	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vuln [illegible]	[illegible]	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16 | 25

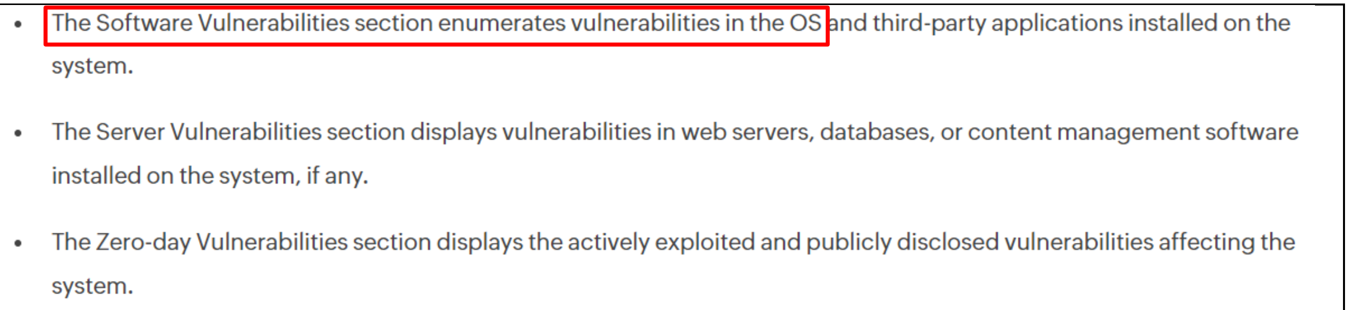
the software listed
next is the vulnerabilities

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

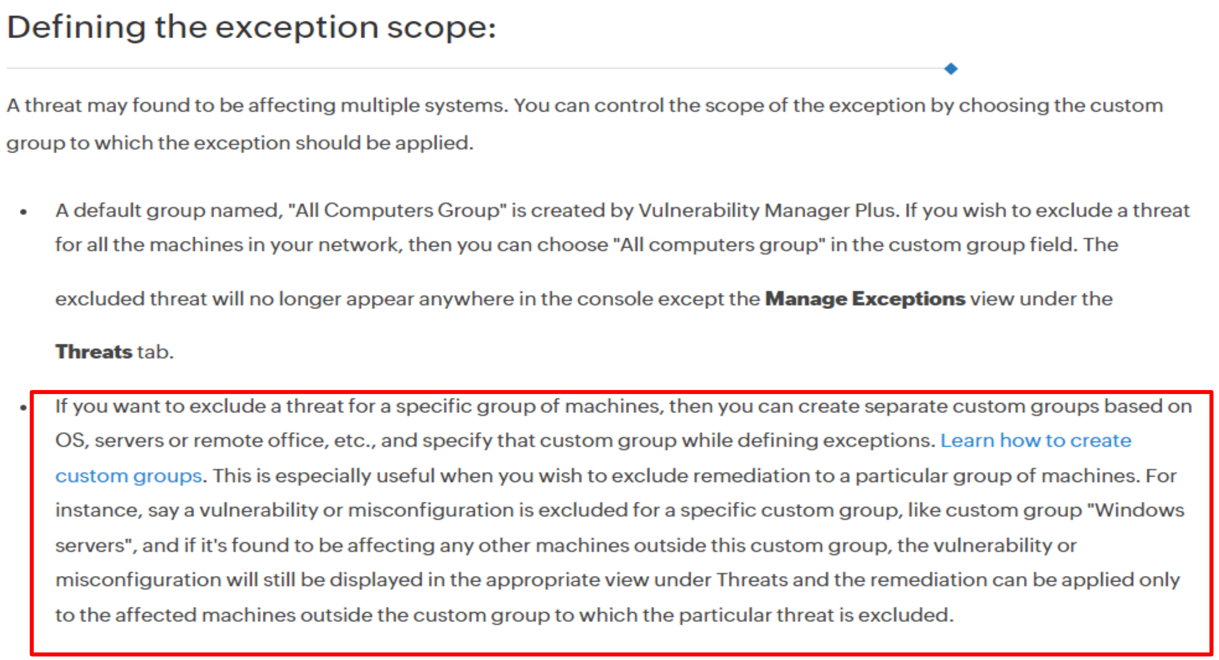
EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html



Defining the exception scope:

A threat may found to be affecting multiple systems. You can control the scope of the exception by choosing the custom group to which the exception should be applied.

- A default group named, "All Computers Group" is created by Vulnerability Manager Plus. If you wish to exclude a threat for all the machines in your network, then you can choose "All computers group" in the custom group field. The excluded threat will no longer appear anywhere in the console except the **Manage Exceptions** view under the **Threats** tab.
- If you want to exclude a threat for a specific group of machines, then you can create separate custom groups based on OS, servers or remote office, etc., and specify that custom group while defining exceptions. Learn how to create custom groups. This is especially useful when you wish to exclude remediation to a particular group of machines. For instance, say a vulnerability or misconfiguration is excluded for a specific custom group, like custom group "Windows servers", and if it's found to be affecting any other machines outside this custom group, the vulnerability or misconfiguration will still be displayed in the appropriate view under Threats and the remediation can be applied only to the affected machines outside the custom group to which the particular threat is excluded.

https://www.manageengine.com/vulnerability-management/help/managing-threat-and-vulnerability-exceptions.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

at the at least one device: receiving, from the at least one server over the at least one network, the first vulnerability information;	ManageEngine, when in operation, practices a method wherein *at least one device* (e.g., any endpoint or client) *receiving, from the at least one server over the at least one network, the first vulnerability information,* (e.g., a Vulnerability Manager Plus server scans the network for software/zero-day vulnerabilities and displays them in a dedicated view in the console on the endpoint or client) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

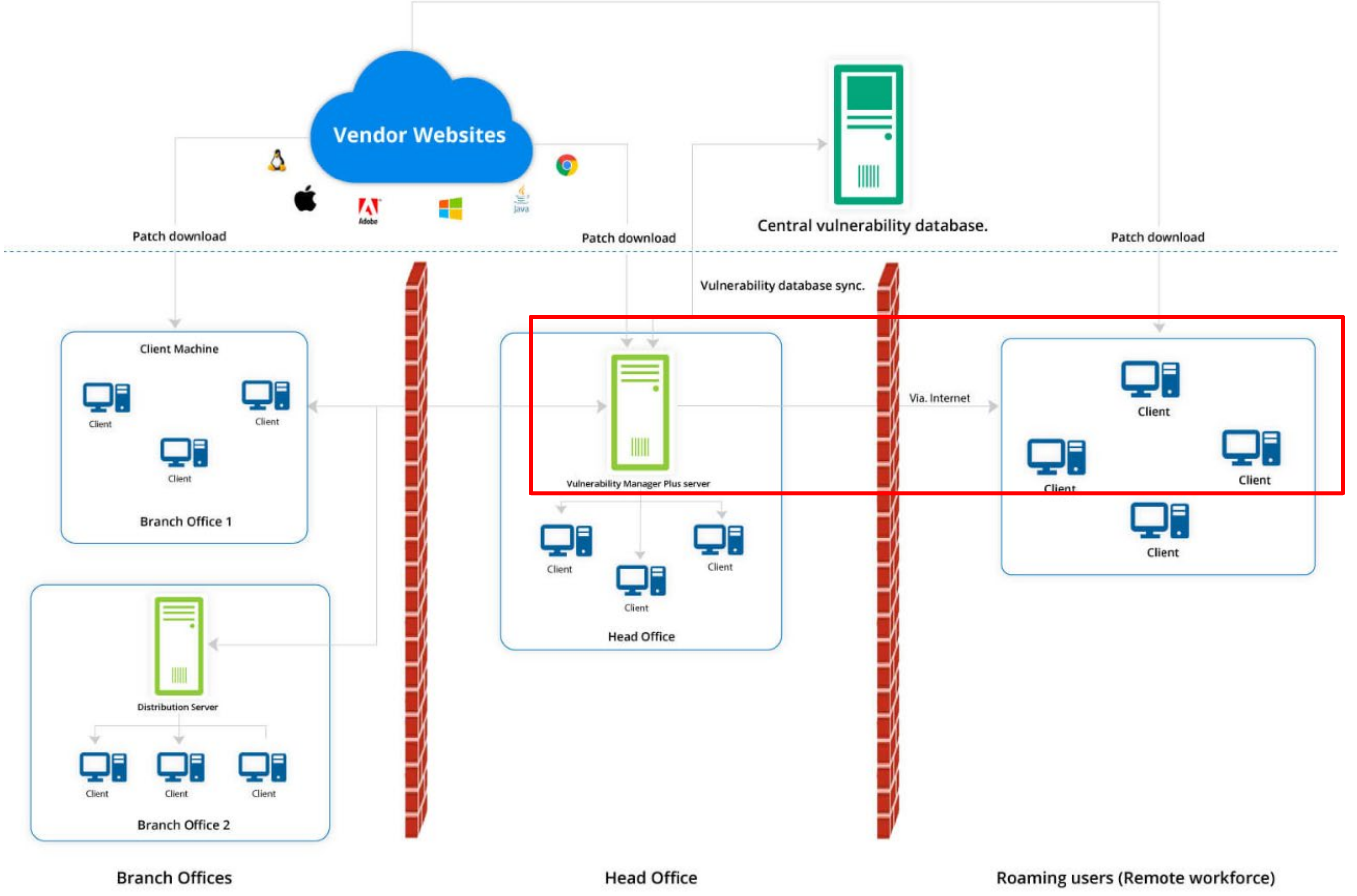
	 Vendor Websites Adobe Java Patch download Patch download Central vulnerability database. Patch download Vulnerability database sync. Client Machine Client Client Client Branch Office 1 Vulnerability Manager Plus server Via. Internet Client Client Client Client Client Client Client Head Office Distribution Server Client Client Client Branch Office 2 Branch Offices Head Office Roaming users (Remote workforce) https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

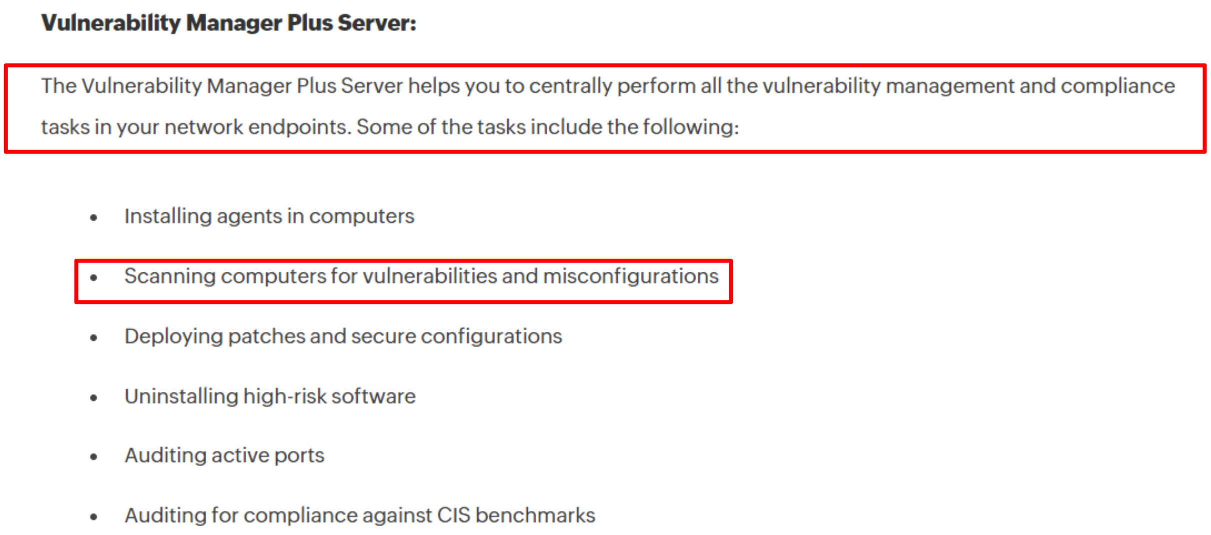
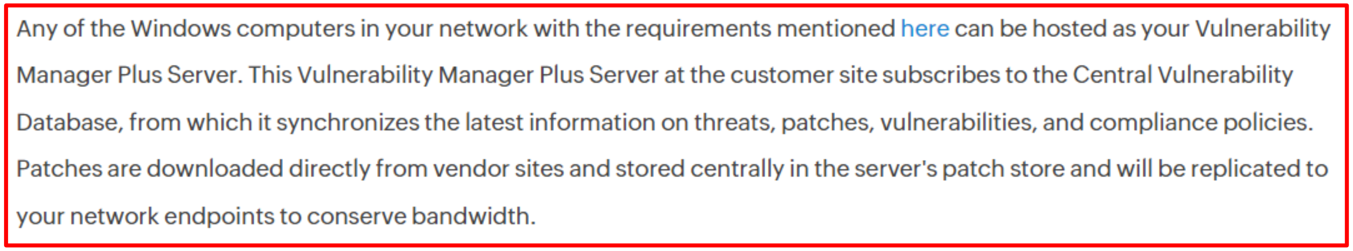
	 **Vulnerability Manager Plus Server:** The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following: • Installing agents in computers • Scanning computers for vulnerabilities and misconfigurations • Deploying patches and secure configurations • Uninstalling high-risk software • Auditing active ports • Auditing for compliance against CIS benchmarks https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html  Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth. https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html

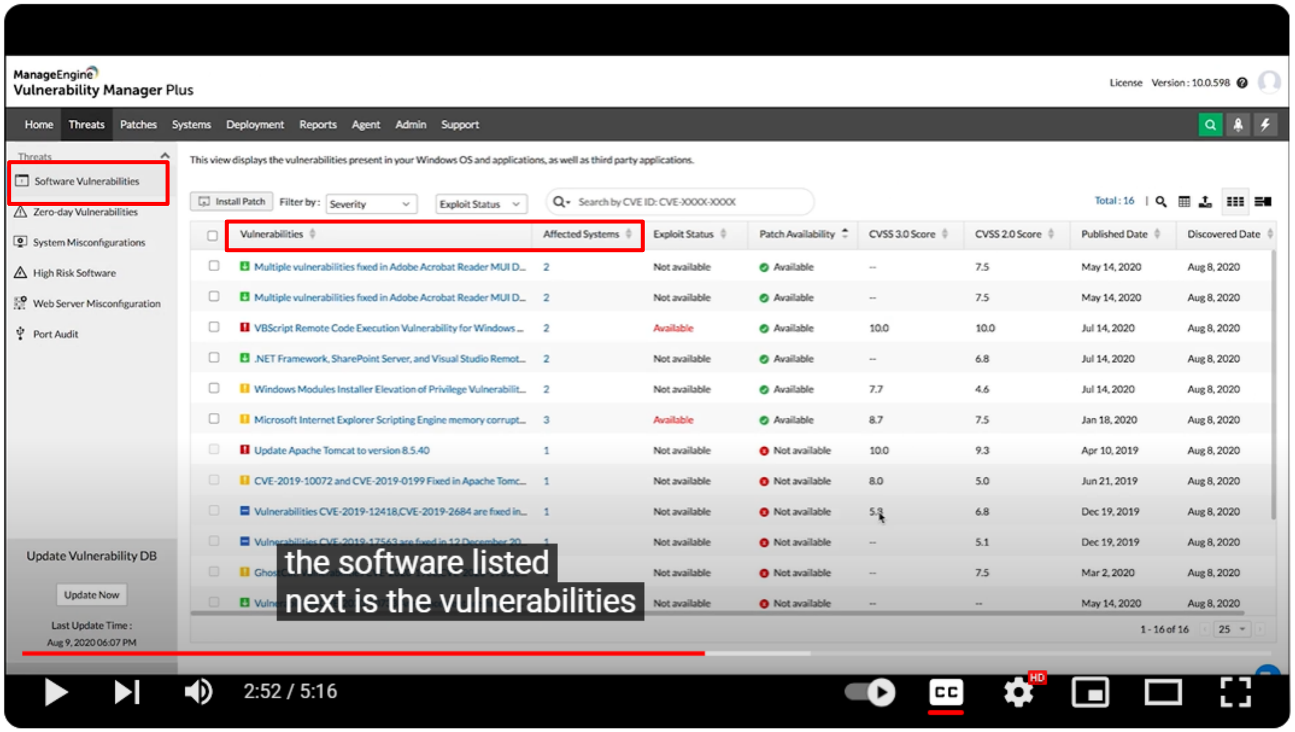
EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

identifying a first portion of the first vulnerability information that includes data inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other data inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	ManageEngine, when in operation, practices a method of *identifying a first portion of the first vulnerability information that includes data inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., software vulnerabilities spot OS vulnerabilities that also includes data-inspected related information such as inspecting files, information in code, scanning the data, virus signatures, virus scanner signatures)*, and that excludes other data inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., software vulnerabilities has an exception section which excludes other data inspection related information as specified in the custom exception group) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



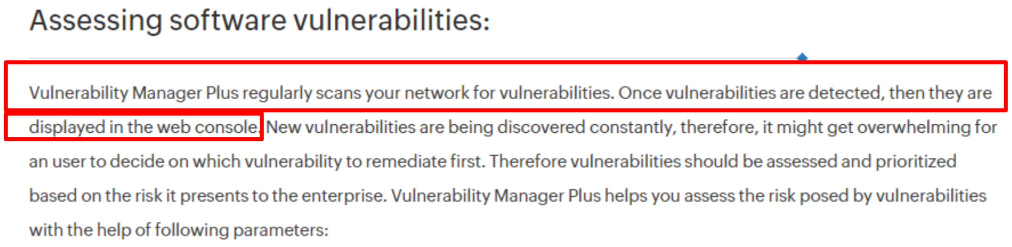
This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

☐	Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
☐	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
☐	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
☐	VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
☐	.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
☐	Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
☐	Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
☐	Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
☐	CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
☐	Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.3	6.8	Dec 19, 2019	Aug 8, 2020
☐	Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
☐	Ghos[illegible]	[illegible]	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
☐	Vuln[illegible]	[illegible]	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

the software listed
next is the vulnerabilities

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA



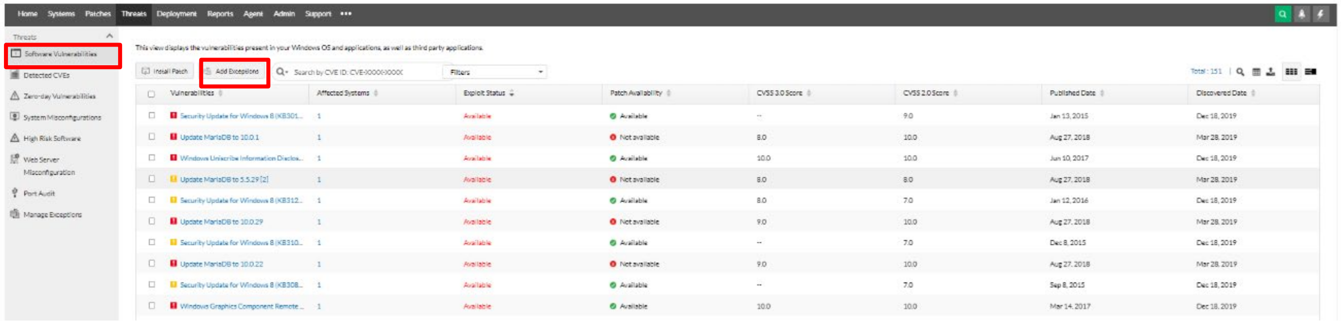
Assessing software vulnerabilities:

Vulnerability Manager Plus regularly scans your network for vulnerabilities. Once vulnerabilities are detected, then they are displayed in the web console. New vulnerabilities are being discovered constantly, therefore, it might get overwhelming for an user to decide on which vulnerability to remediate first. Therefore vulnerabilities should be assessed and prioritized based on the risk it presents to the enterprise. Vulnerability Manager Plus helps you assess the risk posed by vulnerabilities with the help of following parameters:

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td></td>
<td>
https://www.managengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html



This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

<table>
<tr><th>☐</th><th>Vulnerabilities</th><th>Affected Systems</th><th>Exploit Status</th><th>Patch Availability</th><th>CVSS 3.0 Score</th><th>CVSS 2.0 Score</th><th>Published Date</th><th>Discovered Date</th></tr>
<tr><td>☐</td><td>Security Update for Windows 8 (KB301...</td><td>1</td><td>Available</td><td>Available</td><td>--</td><td>9.0</td><td>Jan 13, 2015</td><td>Dec 18, 2019</td></tr>
<tr><td>☐</td><td>Update MariaDB to 10.0.1</td><td>1</td><td>Available</td><td>Not available</td><td>8.0</td><td>10.0</td><td>Aug 27, 2018</td><td>Mar 28, 2019</td></tr>
<tr><td>☐</td><td>Windows Uniscribe Information Disclos...</td><td>1</td><td>Available</td><td>Available</td><td>10.0</td><td>10.0</td><td>Jun 10, 2017</td><td>Dec 18, 2019</td></tr>
<tr><td>☐</td><td>Update MariaDB to 5.5.29 [2]</td><td>1</td><td>Available</td><td>Not available</td><td>8.0</td><td>8.0</td><td>Aug 27, 2018</td><td>Mar 28, 2019</td></tr>
<tr><td>☐</td><td>Security Update for Windows 8 (KB312...</td><td>1</td><td>Available</td><td>Available</td><td>8.0</td><td>7.0</td><td>Jan 12, 2016</td><td>Dec 18, 2019</td></tr>
<tr><td>☐</td><td>Update MariaDB to 10.0.29</td><td>1</td><td>Available</td><td>Not available</td><td>9.0</td><td>10.0</td><td>Aug 27, 2018</td><td>Mar 28, 2019</td></tr>
<tr><td>☐</td><td>Security Update for Windows 8 (KB310...</td><td>1</td><td>Available</td><td>Available</td><td>--</td><td>7.0</td><td>Dec 8, 2015</td><td>Dec 18, 2019</td></tr>
<tr><td>☐</td><td>Update MariaDB to 10.0.22</td><td>1</td><td>Available</td><td>Not available</td><td>9.0</td><td>10.0</td><td>Aug 27, 2018</td><td>Mar 28, 2019</td></tr>
<tr><td>☐</td><td>Security Update for Windows 8 (KB308...</td><td>1</td><td>Available</td><td>Available</td><td>--</td><td>7.0</td><td>Sep 8, 2015</td><td>Dec 18, 2019</td></tr>
<tr><td>☐</td><td>Windows Graphics Component Remote ...</td><td>1</td><td>Available</td><td>Available</td><td>10.0</td><td>10.0</td><td>Mar 14, 2017</td><td>Dec 18, 2019</td></tr>
</table>

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html?wfh-webpage
</td>
</tr>
<tr>
<td>identifying a first event of a plurality of events in connection with the at least one device;
causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is susceptible to being taken</td>
<td>ManageEngine, when in operation, practices a method <em>of identifying a first event of a plurality of events in connection with the at least one device</em> (e.g., event such as remote code execution for windows on window endpoint) <em>causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is susceptible to being taken advantage of by the first event identified in connection with the at least one device, utilizing the data inspection-related information</em> (e.g., event which is provided exploit status as available or severity level as critical indicates that the information is susceptible to being taken advantage of by the event such as remote code execution for windows as shown in the snippet provided)
<strong>Note:</strong> See, for example, the evidence above (where applicable) and below (emphasis added, if any):</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

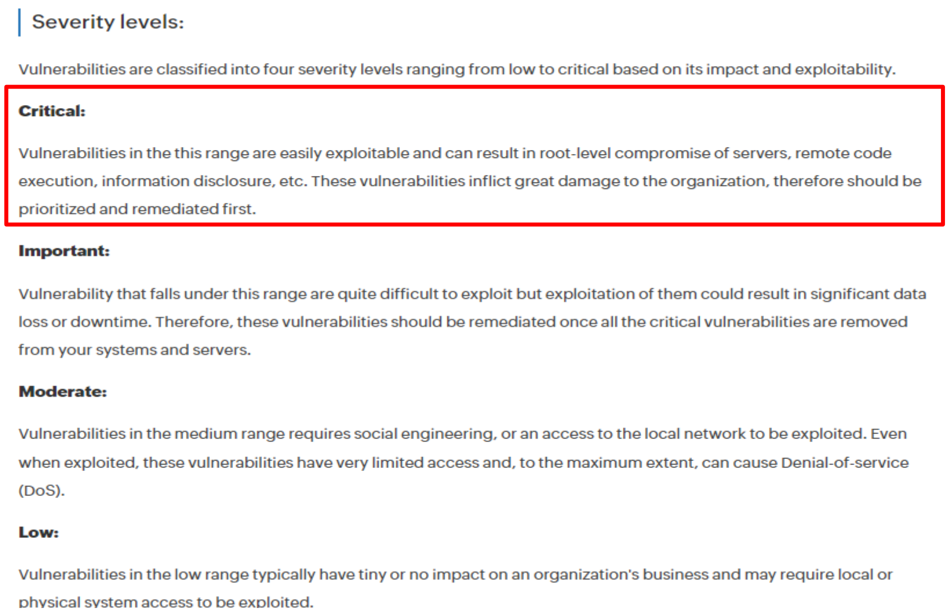
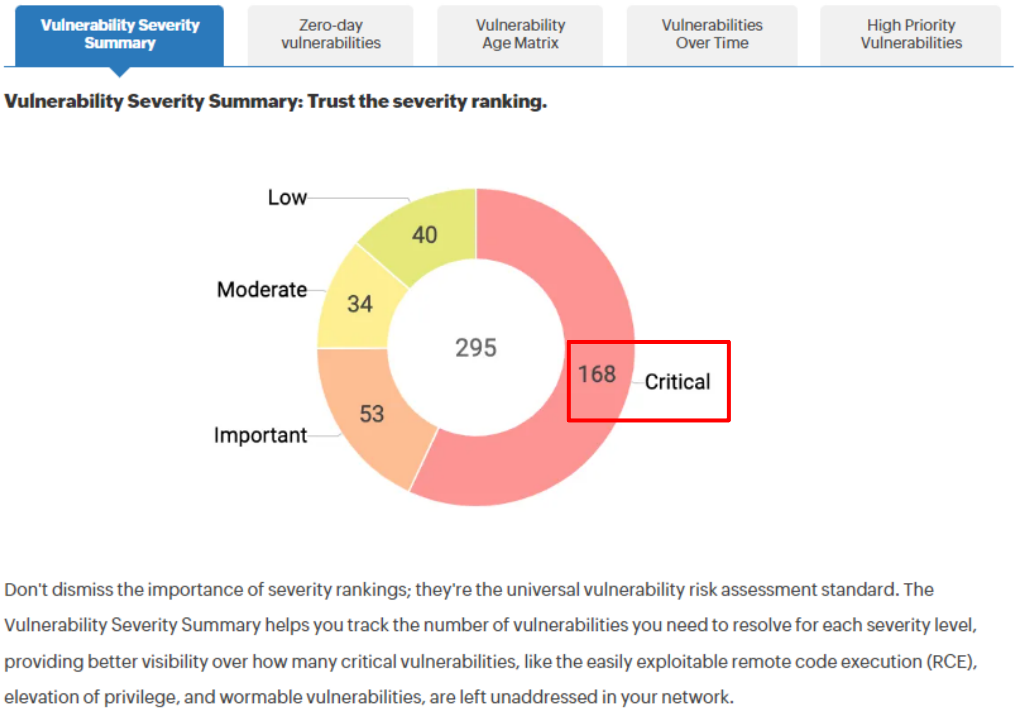
advantage of by the first event identified in connection with the at least one device, utilizing the data inspection-related information;	 Severity levels: Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability. **Critical:** Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first. **Important:** Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers. **Moderate:** Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS). **Low:** Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited. https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

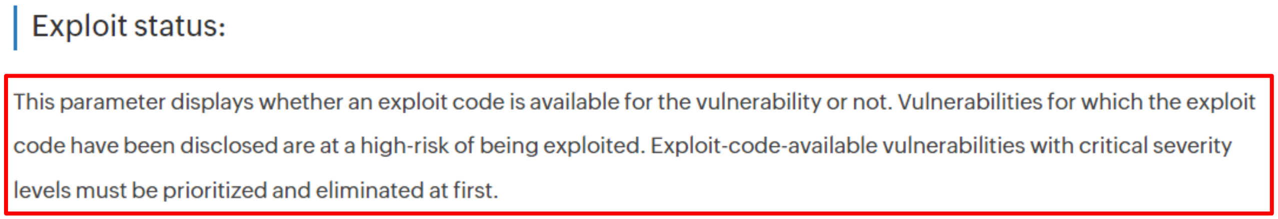
U.S. Patent No 10,873,595 v. Zoho



Vulnerability Severity Summary: Trust the severity ranking.

Don't dismiss the importance of severity rankings; they're the universal vulnerability risk assessment standard. The Vulnerability Severity Summary helps you track the number of vulnerabilities you need to resolve for each severity level, providing better visibility over how many critical vulnerabilities, like the easily exploitable remote code execution (RCE), elevation of privilege, and wormable vulnerabilities, are left unaddressed in your network.

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html



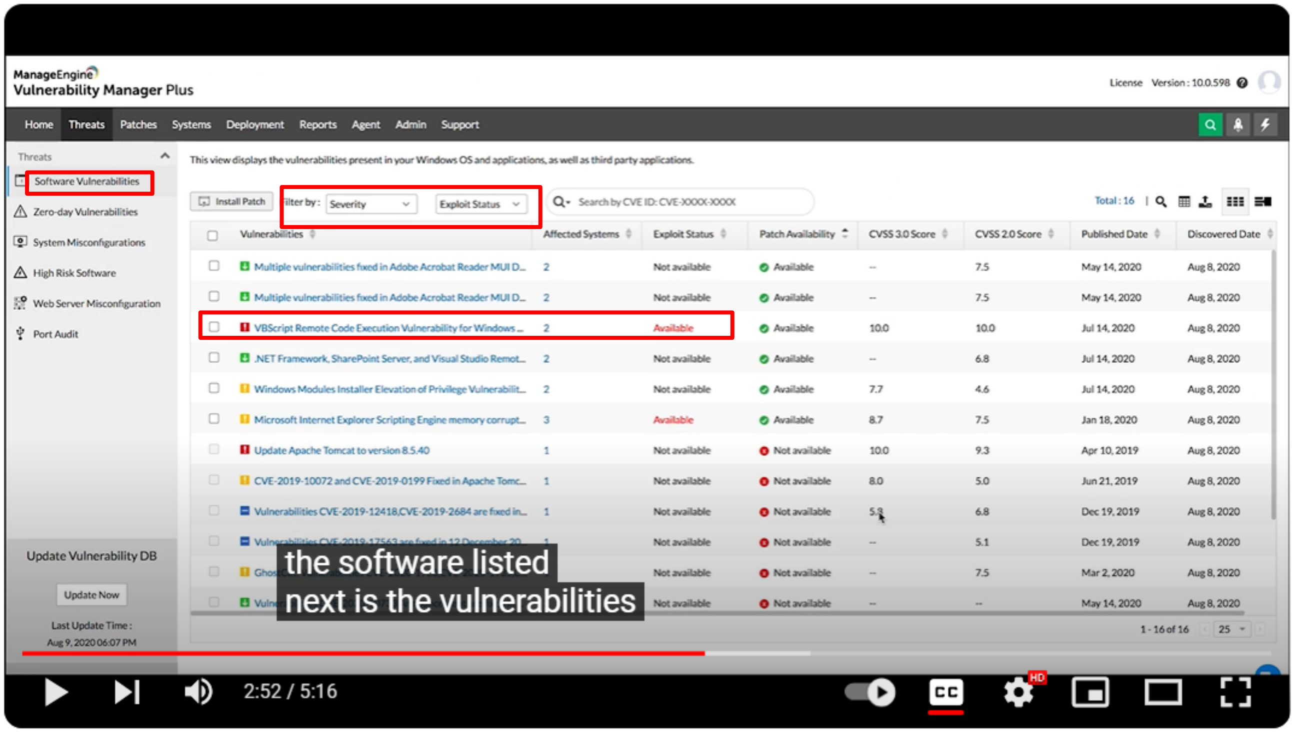
Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

	 **How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus** https://www.youtube.com/watch?v=QfzFLQXNxiA

ManageEngine
Vulnerability Manager Plus

License Version : 10.0.598

Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Filter by : Severity Exploit Status

Search by CVE ID: CVE-XXXX-XXXX

Total : 16

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.3	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
Ghos		Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vuln		Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16

the software listed
next is the vulnerabilities

2:52 / 5:16

identifying a second event of the plurality of events in connection with the at least one device;	ManageEngine, when in operation, practices a method *of identifying a second event of a plurality of events in connection with the at least one device* (e.g., event such as multiple vulnerabilities in Adobe Acrobat) *causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is not susceptible to being taken advantage of by the second event identified*

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

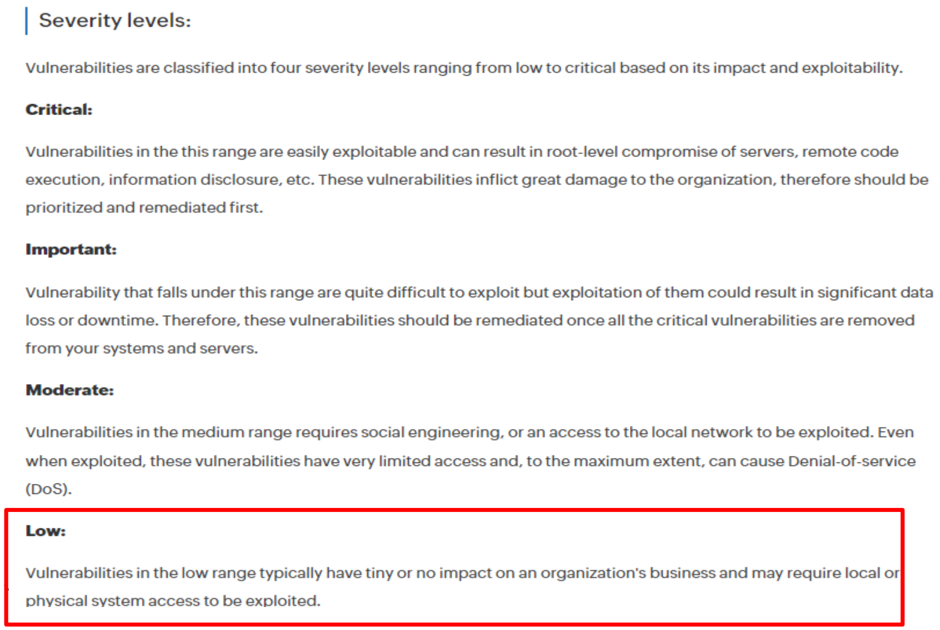
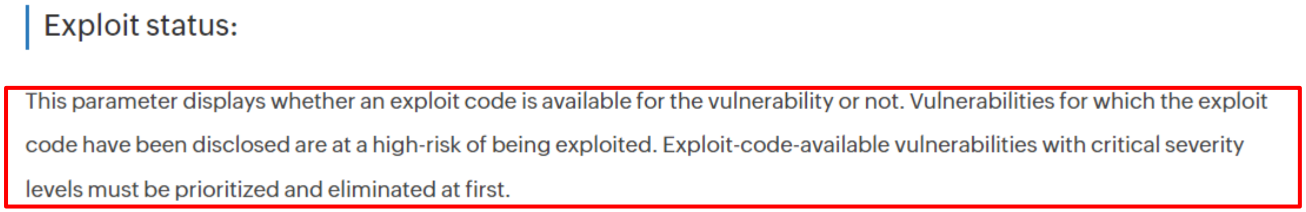
causing a determination that the at least one of the actual vulnerabilities corresponding with the data inspection-related information is not susceptible to being taken advantage of by the second event identified in connection with the at least one device, utilizing the data inspection-related information;	*in connection with the at least one device, utilizing the data inspection-related information* (e.g., event which is provided exploit status as not available or severity level as moderate or low indicates that the information is not susceptible to being taken advantage of by the event such multiple vulnerabilities in Adobe Acrobat as shown in the snippet provided) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  Severity levels: Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability. **Critical:** Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first. **Important:** Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers. **Moderate:** Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS). **Low:** Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited. https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

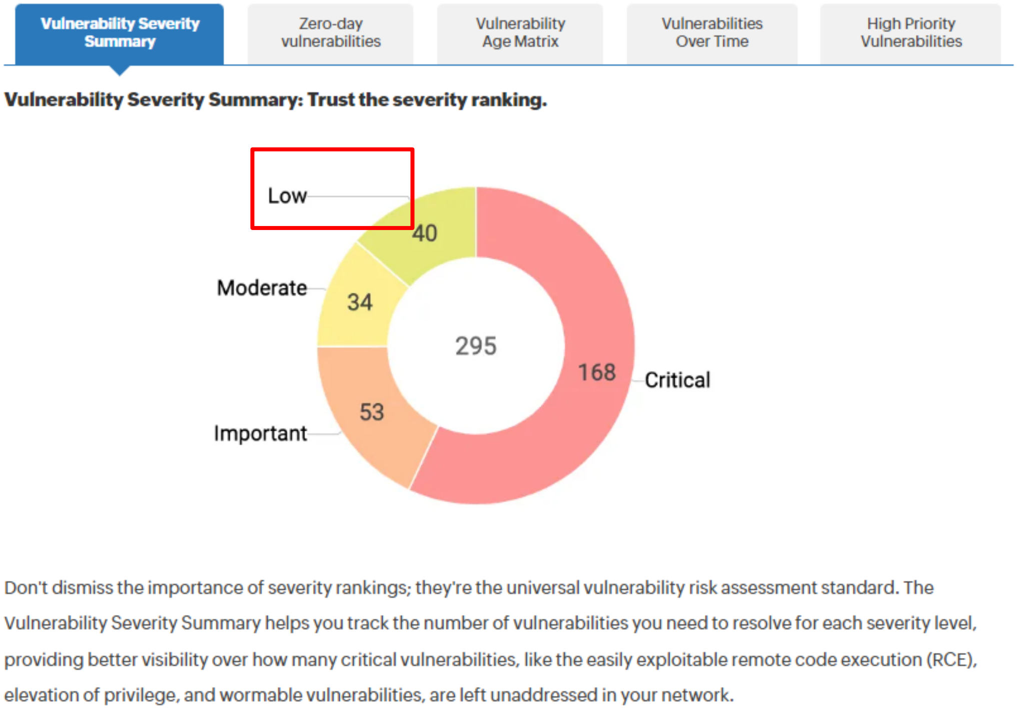
U.S. Patent No 10,873,595 v. Zoho



Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html



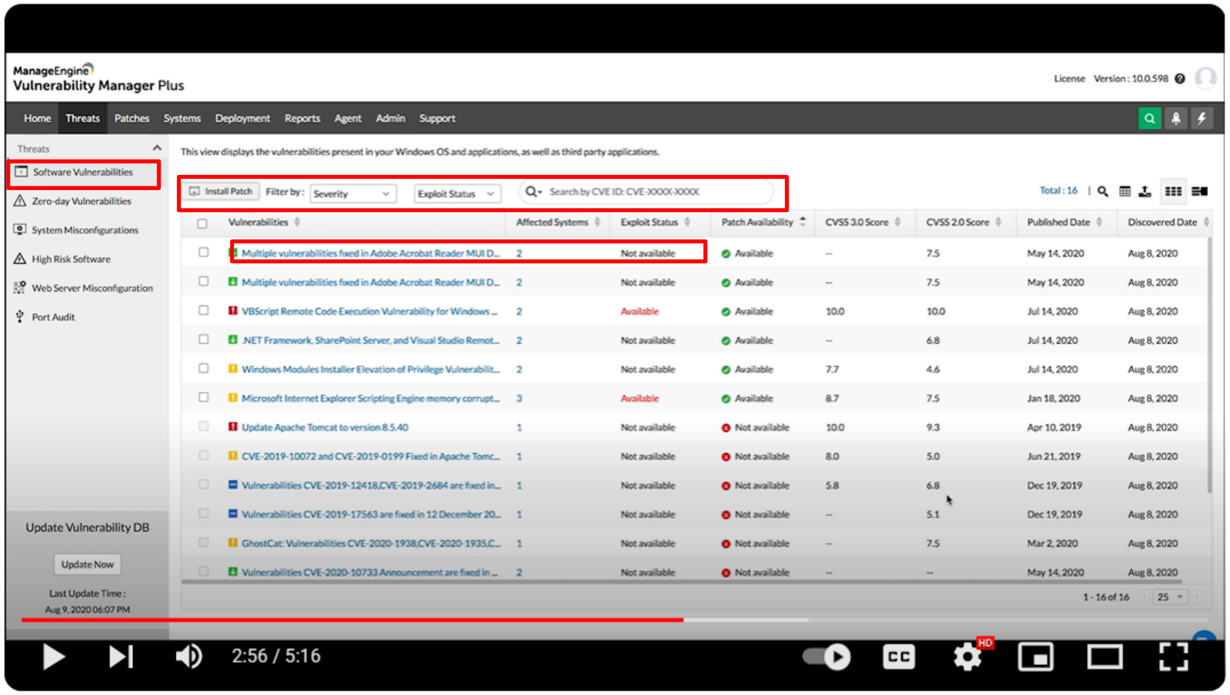
Vulnerability Severity Summary: Trust the severity ranking.

Don't dismiss the importance of severity rankings; they're the universal vulnerability risk assessment standard. The Vulnerability Severity Summary helps you track the number of vulnerabilities you need to resolve for each severity level, providing better visibility over how many critical vulnerabilities, like the easily exploitable remote code execution (RCE), elevation of privilege, and wormable vulnerabilities, are left unaddressed in your network.

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

https://www.managengine.com/vulnerability-management/vulnerability-assessment.html



ManageEngine
Vulnerability Manager Plus

License Version : 10.0.598

Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Filter by : Severity | Exploit Status | Search by CVE ID: CVE-XXXX-XXXX

Total : 16

□	Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
□	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	✓ Available	--	7.5	May 14, 2020	Aug 8, 2020
□	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	✓ Available	--	7.5	May 14, 2020	Aug 8, 2020
□	VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	✓ Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
□	.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	✓ Available	--	6.8	Jul 14, 2020	Aug 8, 2020
□	Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	✓ Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
□	Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	✓ Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
□	Update Apache Tomcat to version 8.5.40	1	Not available	✗ Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
□	CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	✗ Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
□	Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	✗ Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
□	Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	✗ Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
□	GhostCat: Vulnerabilities CVE-2020-1938,CVE-2020-1935,C...	1	Not available	✗ Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
□	Vulnerabilities CVE-2020-10733 Announcement are fixed in ...	2	Not available	✗ Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16 | 25

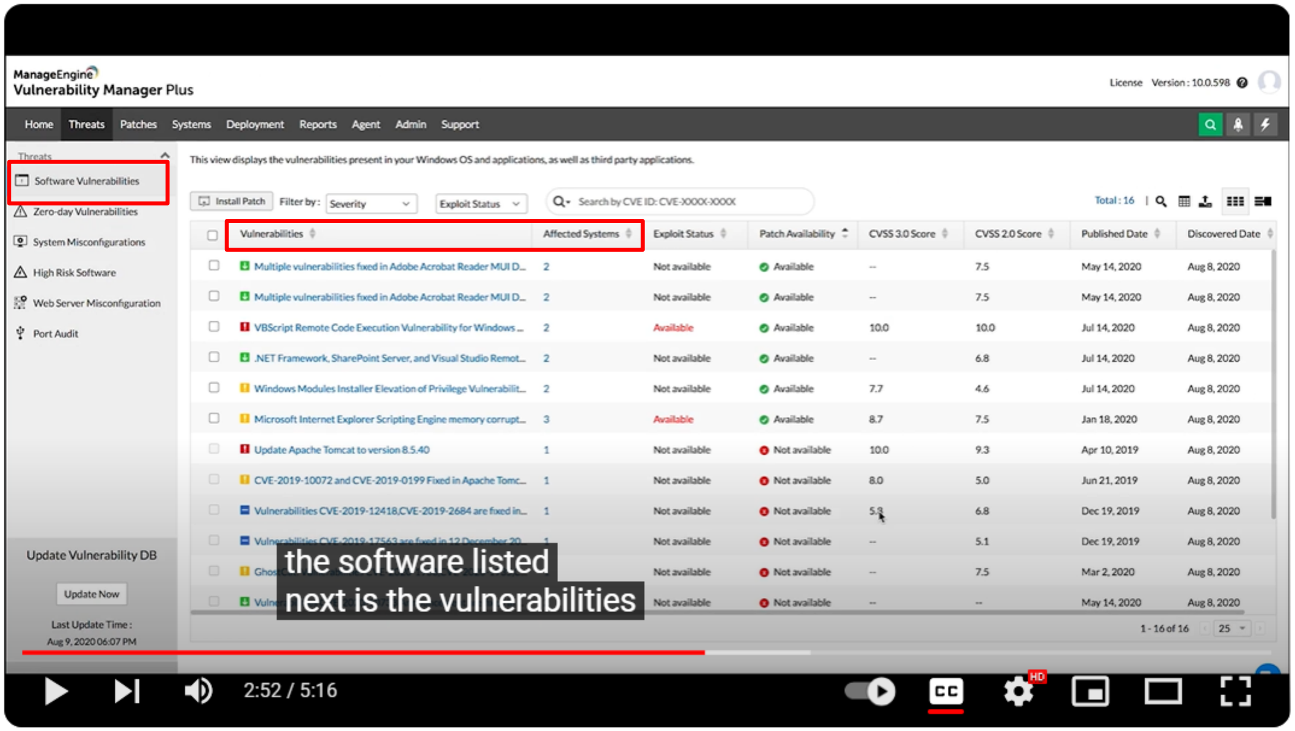
How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

identifying a second portion of the first vulnerability information that includes traffic inspection-related information that corresponds	ManageEngine, when in operation, practices a method of *identifying a second portion of the first vulnerability information that includes traffic inspection-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., software vulnerabilities spot OS vulnerabilities that also includes traffic inspection related information such as host-instruction detection signatures, inspecting traffic for attacks, host-based intrusion detection), *and that*

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

with at least one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other traffic inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;	*excludes other traffic inspection-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., software vulnerabilities has an exception section which excludes other traffic inspection related information as specified in the custom exception group) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

ManageEngine Vulnerability Manager Plus

License Version : 10.0.598

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Filter by : Severity Exploit Status Search by CVE ID: CVE-XXXX-XXXX Total : 16

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
Ghos		Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vuln		Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16 25

Update Vulnerability DB

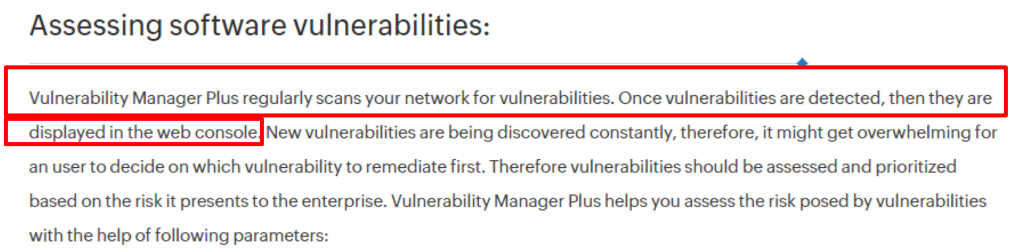
Last Update Time : Aug 9, 2020 06:07 PM

the software listed
next is the vulnerabilities

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

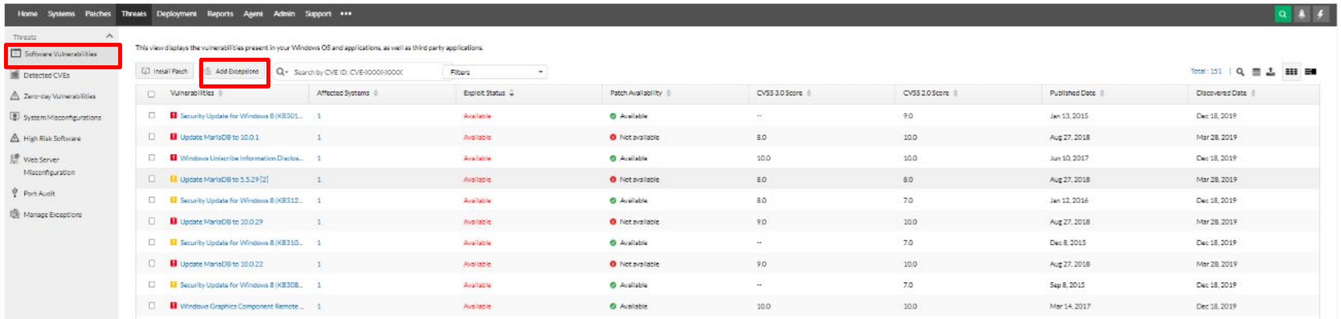
https://www.youtube.com/watch?v=QfzFLQXNxiA



Assessing software vulnerabilities:

Vulnerability Manager Plus regularly scans your network for vulnerabilities. Once vulnerabilities are detected, then they are displayed in the web console. New vulnerabilities are being discovered constantly, therefore, it might get overwhelming for an user to decide on which vulnerability to remediate first. Therefore vulnerabilities should be assessed and prioritized based on the risk it presents to the enterprise. Vulnerability Manager Plus helps you assess the risk posed by vulnerabilities with the help of following parameters:

https://www.managengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html



This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

□	Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
□	Security Update for Windows 8 (KB301...	1	Available	Available	--	9.0	Jan 13, 2015	Dec 18, 2019
□	Update MariaDB to 10.0.1	1	Available	Not available	8.0	10.0	Aug 27, 2018	Mar 28, 2019
□	Windows Uniscribe Information Disclos...	1	Available	Available	10.0	10.0	Jun 10, 2017	Dec 18, 2019
□	Update MariaDB to 5.5.29 [2]	1	Available	Not available	8.0	8.0	Aug 27, 2018	Mar 28, 2019
□	Security Update for Windows 8 (KB312...	1	Available	Available	8.0	7.0	Jan 12, 2016	Dec 18, 2019
□	Update MariaDB to 10.0.29	1	Available	Not available	9.0	10.0	Aug 27, 2018	Mar 28, 2019
□	Security Update for Windows 8 (KB310...	1	Available	Available	--	7.0	Dec 8, 2015	Dec 18, 2019
□	Update MariaDB to 10.0.22	1	Available	Not available	9.0	10.0	Aug 27, 2018	Mar 28, 2019
□	Security Update for Windows 8 (KB308...	1	Available	Available	--	7.0	Sep 8, 2015	Dec 18, 2019
□	Windows Graphics Component Remote ...	1	Available	Available	10.0	10.0	Mar 14, 2017	Dec 18, 2019

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html?wfh-webpage

identifying a third event of the plurality of events in connection with the at least one device;	ManageEngine, when in operation, practices a method *of identifying a third event of the plurality of events in connection with the at least one device* (e.g., event such as Ghostcat vulnerabilities) *causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is susceptible to being taken advantage of by the third event identified in connection*

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

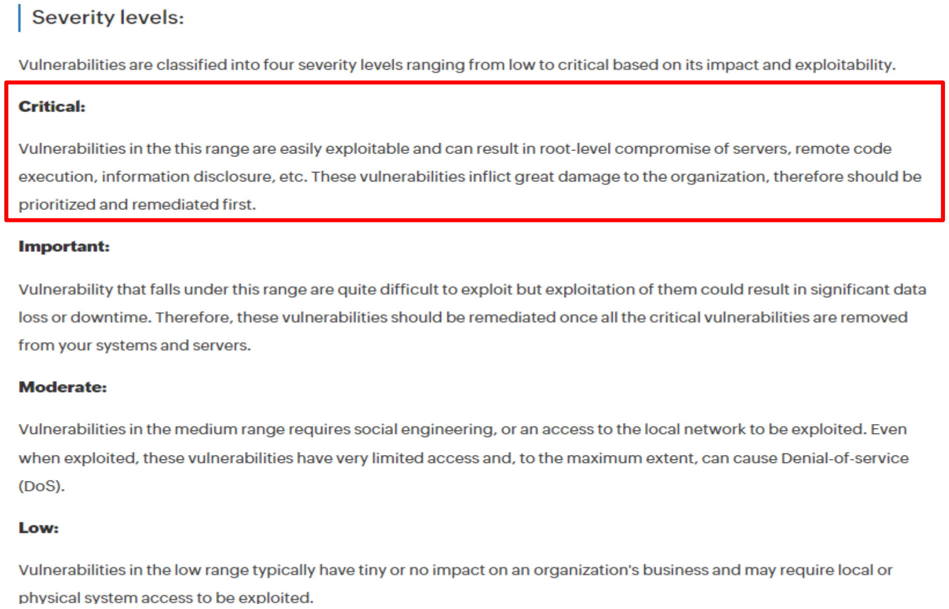
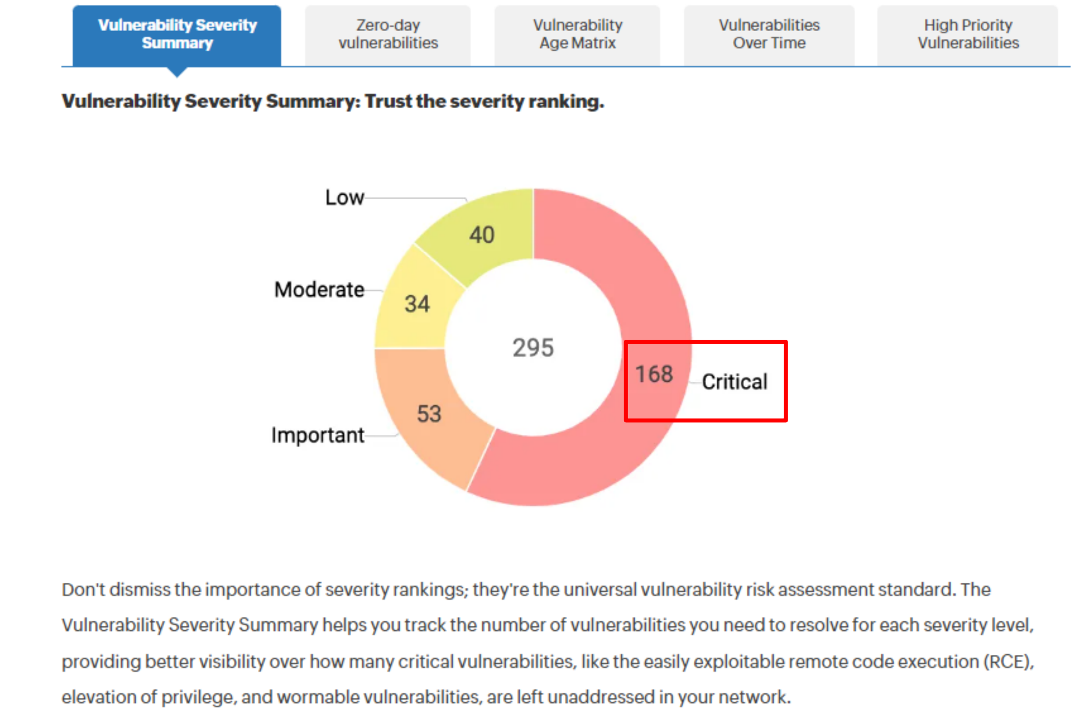
causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is susceptible to being taken advantage of by the third event identified in connection with the at least one device, utilizing the traffic inspection-related information;	*with the at least one device, utilizing the traffic inspection-related information* (e.g., event which is provided exploit status as available or severity level as critical indicates that the information is susceptible to being taken advantage of by the event such as Ghostcat vulnerabilities as shown in the snippet provided. Ghostcat vulnerability which is a high-risk vulnerability and herein attacker may execute malicious code on the target host) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  Severity levels: Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability. **Critical:** Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first. **Important:** Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers. **Moderate:** Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS). **Low:** Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited. https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

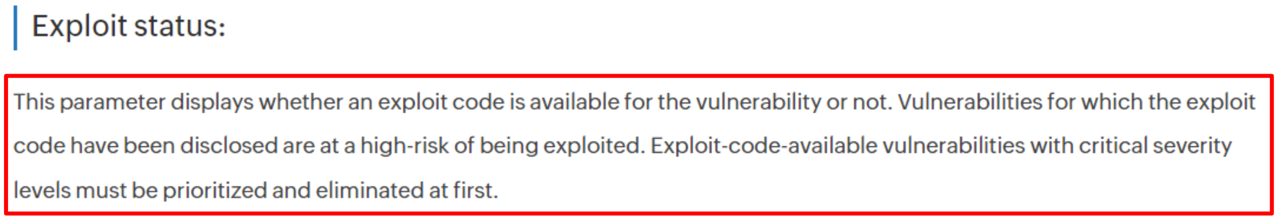
U.S. Patent No 10,873,595 v. Zoho



Vulnerability Severity Summary: Trust the severity ranking.

Don't dismiss the importance of severity rankings; they're the universal vulnerability risk assessment standard. The Vulnerability Severity Summary helps you track the number of vulnerabilities you need to resolve for each severity level, providing better visibility over how many critical vulnerabilities, like the easily exploitable remote code execution (RCE), elevation of privilege, and wormable vulnerabilities, are left unaddressed in your network.

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html



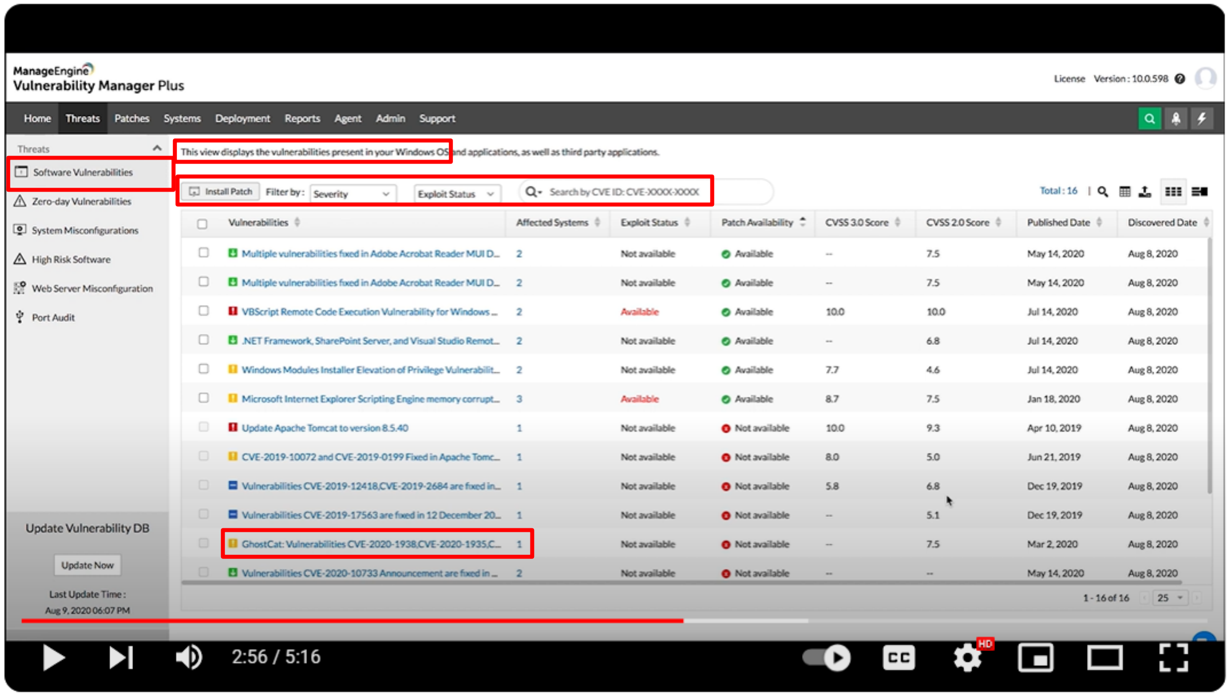
Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho



Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

□	Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
□	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
□	Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
□	VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
□	.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
□	Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
□	Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
□	Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
□	CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
□	Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
□	Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
□	GhostCat: Vulnerabilities CVE-2020-1938,CVE-2020-1935,C...	1	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
□	Vulnerabilities CVE-2020-10733 Announcement are fixed in ...	2	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16 25

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

identifying a fourth event of the plurality of events in connection with the at least one device;	ManageEngine, when in operation, practices a method of *identifying a fourth event of the plurality of events in connection with the at least one device* (e.g., event such as NET framework, share point server) *causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is not susceptible to being taken advantage of by the fourth event identified in connection with the at least one device, utilizing the traffic inspection-related information* (e.g., event which

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

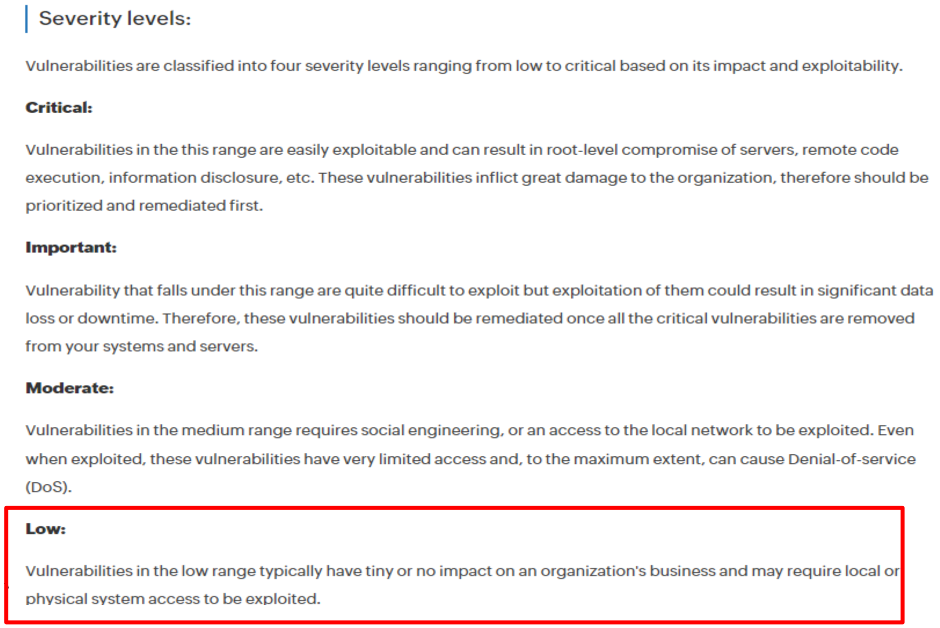
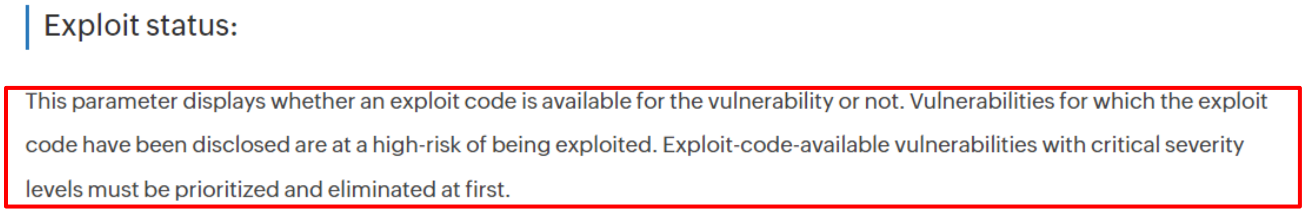
causing a determination that the at least one of the actual vulnerabilities corresponding with the traffic inspection-related information is not susceptible to being taken advantage of by the fourth event identified in connection with the at least one device, utilizing the traffic inspection-related information;	is provided exploit status as not available or severity level as moderate or low indicates that the information is not susceptible to being taken advantage of by the event such as NET framework, share point server as shown in the snippet provided) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  Severity levels: Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability. **Critical:** Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first. **Important:** Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers. **Moderate:** Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS). **Low:** Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited. https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html

EXHIBIT 10

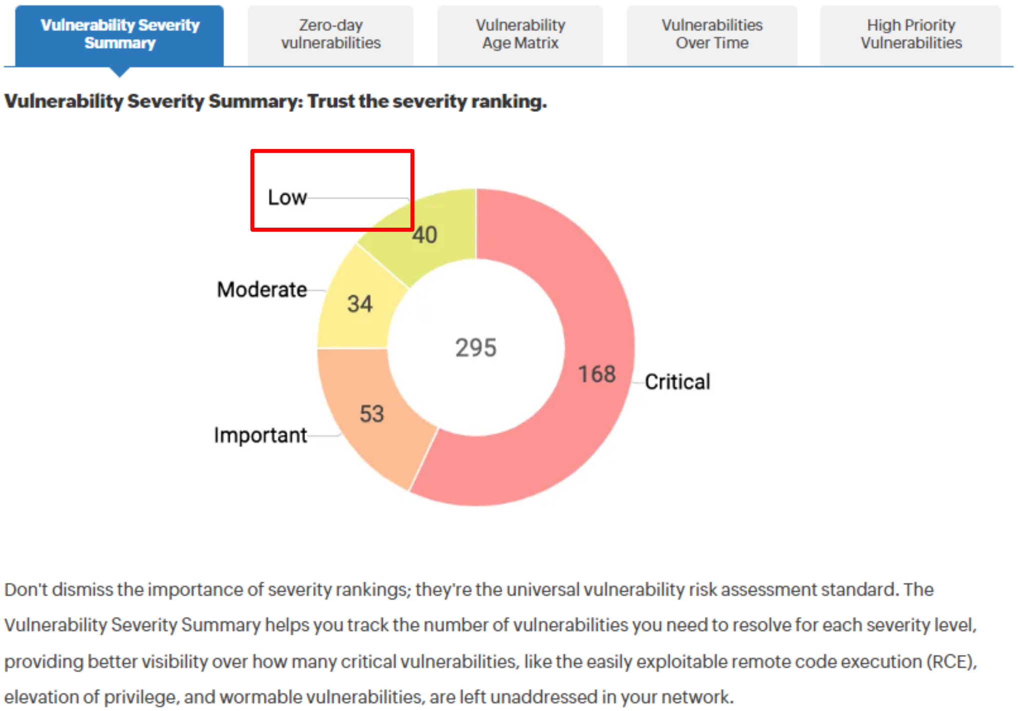
U.S. Patent No 10,873,595 v. Zoho



Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html



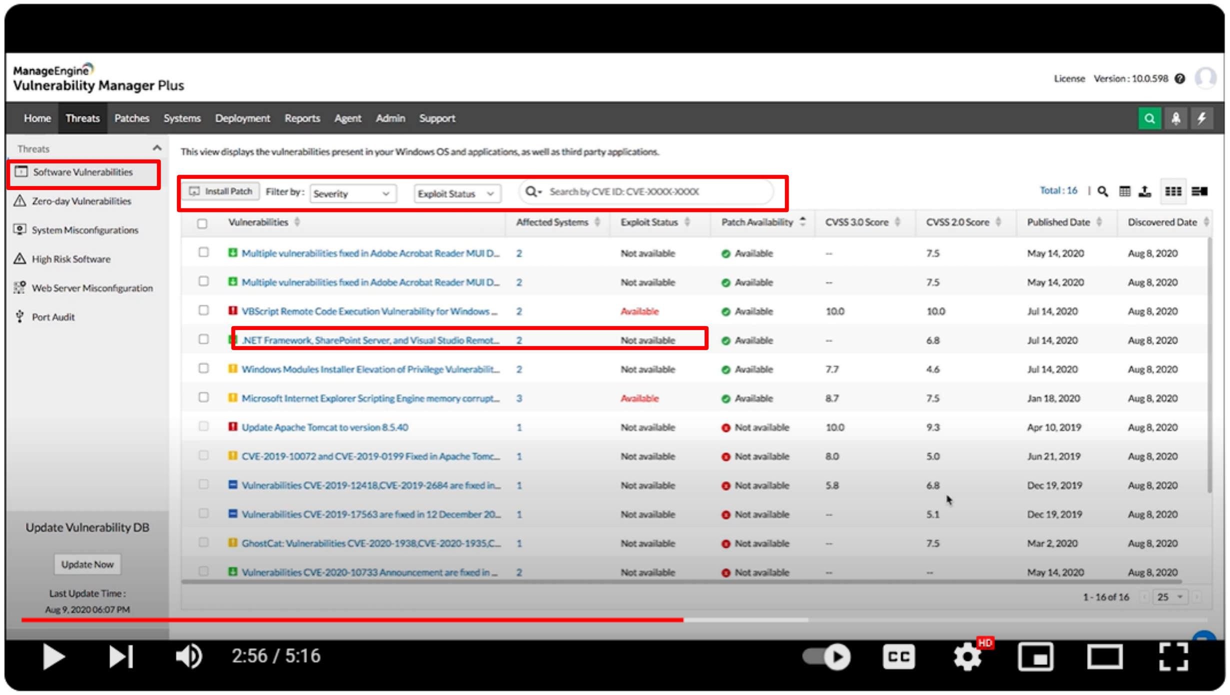
Vulnerability Severity Summary: Trust the severity ranking.

Don't dismiss the importance of severity rankings; they're the universal vulnerability risk assessment standard. The Vulnerability Severity Summary helps you track the number of vulnerabilities you need to resolve for each severity level, providing better visibility over how many critical vulnerabilities, like the easily exploitable remote code execution (RCE), elevation of privilege, and wormable vulnerabilities, are left unaddressed in your network.

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html



ManageEngine Vulnerability Manager Plus

Last Update Time : Aug 9, 2020 06:07 PM

This view displays the vulnerabilities present in your Windows OS and applications, as well as third party applications.

Filter by : Severity · Exploit Status · Search by CVE ID: CVE-XXXX-XXXX · Total : 16

Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
Multiple vulnerabilities fixed in Adobe Acrobat Reader MUI D...	2	Not available	Available	--	7.5	May 14, 2020	Aug 8, 2020
VBScript Remote Code Execution Vulnerability for Windows ...	2	Available	Available	10.0	10.0	Jul 14, 2020	Aug 8, 2020
.NET Framework, SharePoint Server, and Visual Studio Remot...	2	Not available	Available	--	6.8	Jul 14, 2020	Aug 8, 2020
Windows Modules Installer Elevation of Privilege Vulnerabilit...	2	Not available	Available	7.7	4.6	Jul 14, 2020	Aug 8, 2020
Microsoft Internet Explorer Scripting Engine memory corrupt...	3	Available	Available	8.7	7.5	Jan 18, 2020	Aug 8, 2020
Update Apache Tomcat to version 8.5.40	1	Not available	Not available	10.0	9.3	Apr 10, 2019	Aug 8, 2020
CVE-2019-10072 and CVE-2019-0199 Fixed in Apache Tomc...	1	Not available	Not available	8.0	5.0	Jun 21, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-12418,CVE-2019-2684 are fixed in...	1	Not available	Not available	5.8	6.8	Dec 19, 2019	Aug 8, 2020
Vulnerabilities CVE-2019-17563 are fixed in 12 December 20...	1	Not available	Not available	--	5.1	Dec 19, 2019	Aug 8, 2020
GhostCat: Vulnerabilities CVE-2020-1938,CVE-2020-1935,C...	1	Not available	Not available	--	7.5	Mar 2, 2020	Aug 8, 2020
Vulnerabilities CVE-2020-10733 Announcement are fixed in ...	2	Not available	Not available	--	--	May 14, 2020	Aug 8, 2020

1 - 16 of 16 · 25

How to do Vulnerability Assessment with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=QfzFLQXNxiA

identifying a third portion of the first vulnerability information that includes firewall-related information that corresponds with at least	ManageEngine, when in operation, practices a method of *identifying a third portion of the first vulnerability information that includes firewall-related information that corresponds with at least one of the actual vulnerabilities of the at least one operating system of the at least one device* (e.g., security misconfiguration provide vulnerability information that includes to firewall related information on the windows system), *and that excludes other traffic inspection-related information of the second vulnerability information that does*

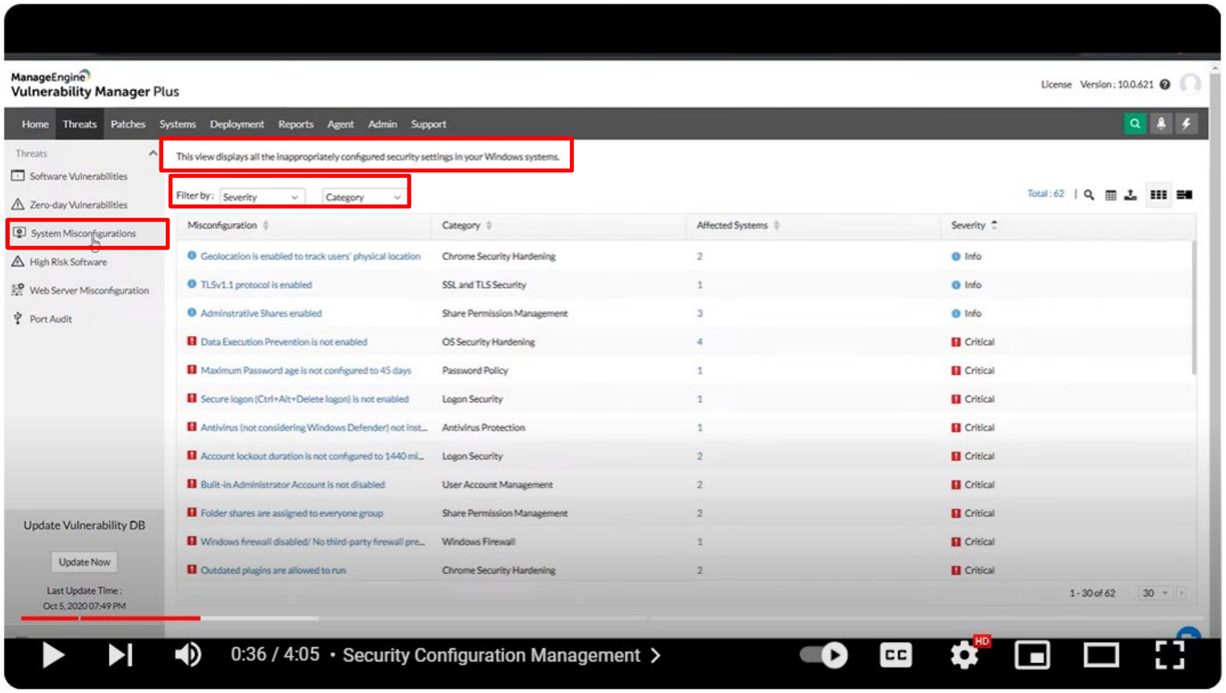
EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td>one of the actual vulnerabilities of the at least one operating system of the at least one device, and that excludes other firewall-related information of the second vulnerability information that does not correspond with the actual vulnerabilities of the at least one operating system of the at least one device;</td>
<td>

not correspond with the actual vulnerabilities of the at least one operating system of the at least one device (e.g., by providing the exception scope the custom groups vulnerability or misconfiguration can be excluded)

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):



ManageEngine Vulnerability Manager Plus

License Version : 10.0.621

This view displays all the inappropriately configured security settings in your Windows systems.

Filter by : Severity Category

Total : 62

<table>
<tr><th>Misconfiguration</th><th>Category</th><th>Affected Systems</th><th>Severity</th></tr>
<tr><td>Geolocation is enabled to track users' physical location</td><td>Chrome Security Hardening</td><td>2</td><td>Info</td></tr>
<tr><td>TLSv1.1 protocol is enabled</td><td>SSL and TLS Security</td><td>1</td><td>Info</td></tr>
<tr><td>Adminstrative Shares enabled</td><td>Share Permission Management</td><td>3</td><td>Info</td></tr>
<tr><td>Data Execution Prevention is not enabled</td><td>OS Security Hardening</td><td>4</td><td>Critical</td></tr>
<tr><td>Maximum Password age is not configured to 45 days</td><td>Password Policy</td><td>1</td><td>Critical</td></tr>
<tr><td>Secure logon (Ctrl+Alt+Delete logon) is not enabled</td><td>Logon Security</td><td>1</td><td>Critical</td></tr>
<tr><td>Antivirus (not considering Windows Defender) not inst...</td><td>Antivirus Protection</td><td>1</td><td>Critical</td></tr>
<tr><td>Account lockout duration is not configured to 1440 mi...</td><td>Logon Security</td><td>2</td><td>Critical</td></tr>
<tr><td>Built-in Administrator Account is not disabled</td><td>User Account Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Folder shares are assigned to everyone group</td><td>Share Permission Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Windows firewall disabled/ No third-party firewall pre...</td><td>Windows Firewall</td><td>1</td><td>Critical</td></tr>
<tr><td>Outdated plugins are allowed to run</td><td>Chrome Security Hardening</td><td>2</td><td>Critical</td></tr>
</table>

1 - 30 of 62 30

Update Vulnerability DB

Last Update Time : Oct 5, 2020 07:49 PM

0:36 / 4:05 • Security Configuration Management

Security Configuration Management with ManageEngine Vulnerability Manager Plus

</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

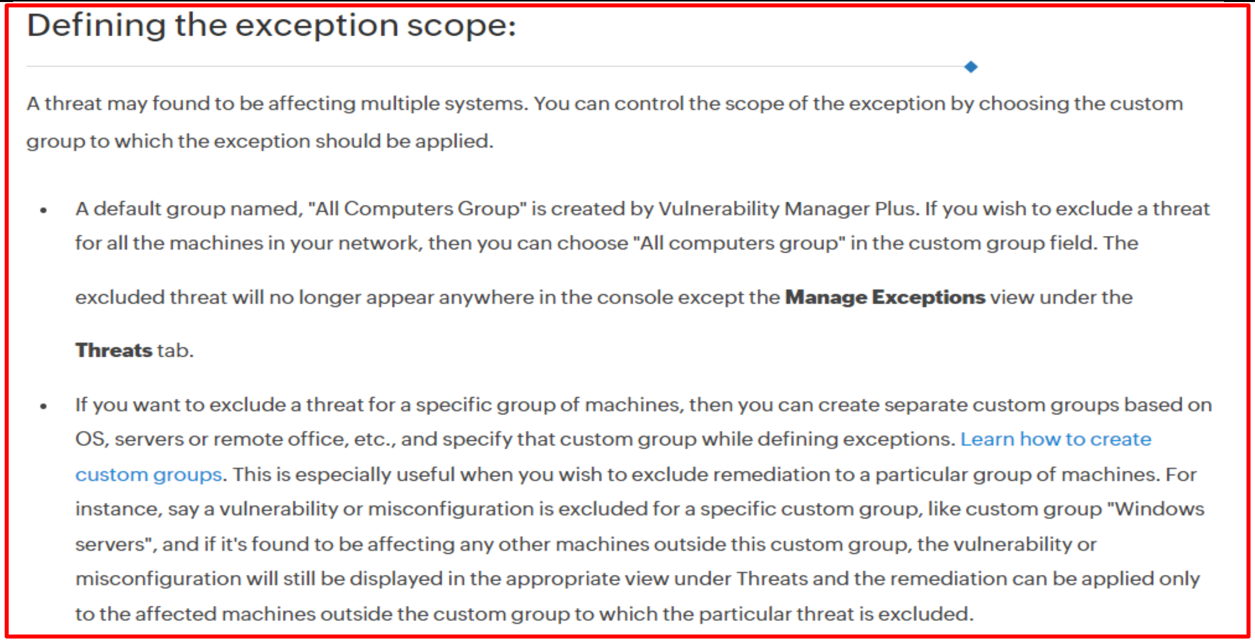
	 Defining the exception scope: A threat may found to be affecting multiple systems. You can control the scope of the exception by choosing the custom group to which the exception should be applied. - A default group named, "All Computers Group" is created by Vulnerability Manager Plus. If you wish to exclude a threat for all the machines in your network, then you can choose "All computers group" in the custom group field. The excluded threat will no longer appear anywhere in the console except the **Manage Exceptions** view under the **Threats** tab. - If you want to exclude a threat for a specific group of machines, then you can create separate custom groups based on OS, servers or remote office, etc., and specify that custom group while defining exceptions. Learn how to create custom groups. This is especially useful when you wish to exclude remediation to a particular group of machines. For instance, say a vulnerability or misconfiguration is excluded for a specific custom group, like custom group "Windows servers", and if it's found to be affecting any other machines outside this custom group, the vulnerability or misconfiguration will still be displayed in the appropriate view under Threats and the remediation can be applied only to the affected machines outside the custom group to which the particular threat is excluded. https://www.manageengine.com/vulnerability-management/help/managing-threat-and-vulnerability-exceptions.html
identifying a fifth event of the plurality of events in connection with the at least one device; causing a determination that the at least one of the actual	ManageEngine, when in operation, practices a method of *identifying a fifth event of the plurality of events in connection with the at least one device* (e.g., event such as windows firewall disabled) *causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is susceptible to being taken advantage of by the fifth event identified in connection with the at least one device, utilizing the firewall-related information* (e.g., event which is provided category as firewall

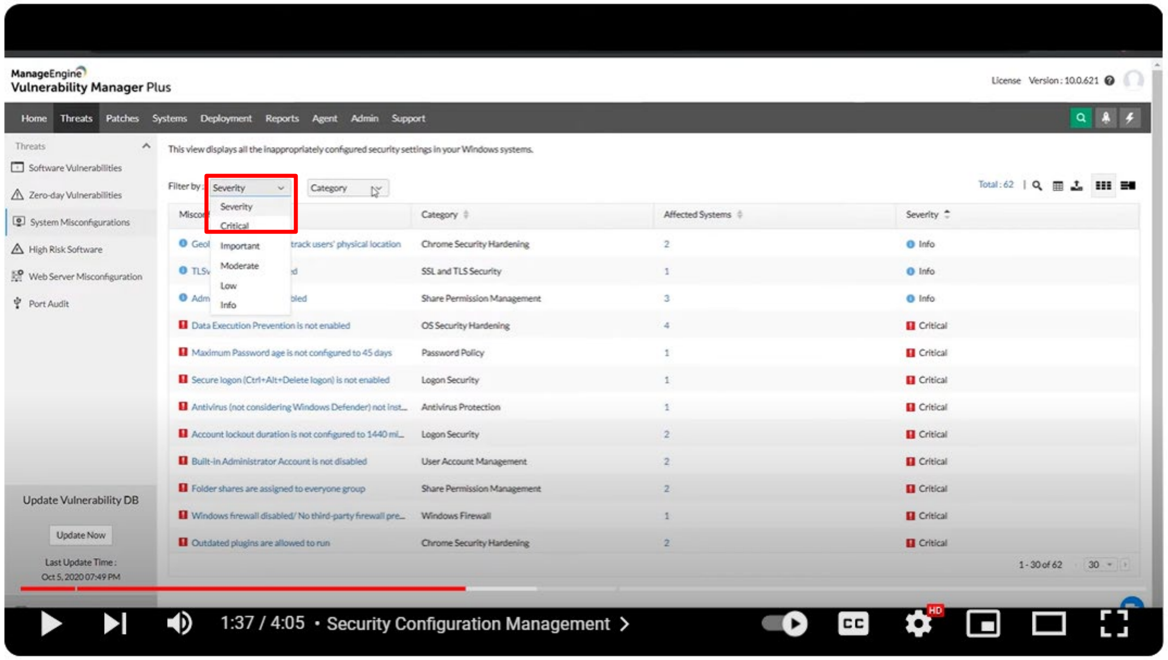
EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

vulnerabilities corresponding with the firewall-related information is susceptible to being taken advantage of by the fifth event identified in connection with the at least one device, utilizing the firewall-related information;

and the severity level as critical indicates that the information is susceptible to being taken advantage of by the event such windows firewall disabled as shown in the snippet provided)

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):



This view displays all the inappropriately configured security settings in your Windows systems.

Last Update Time : Oct 5, 2020 07:49 PM

Miscon	Category	Affected Systems	Severity
Geol … track users' physical location	Chrome Security Hardening	2	Info
TLSv … d	SSL and TLS Security	1	Info
Adm … bled	Share Permission Management	3	Info
Data Execution Prevention is not enabled	OS Security Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not inst...	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 mi...	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

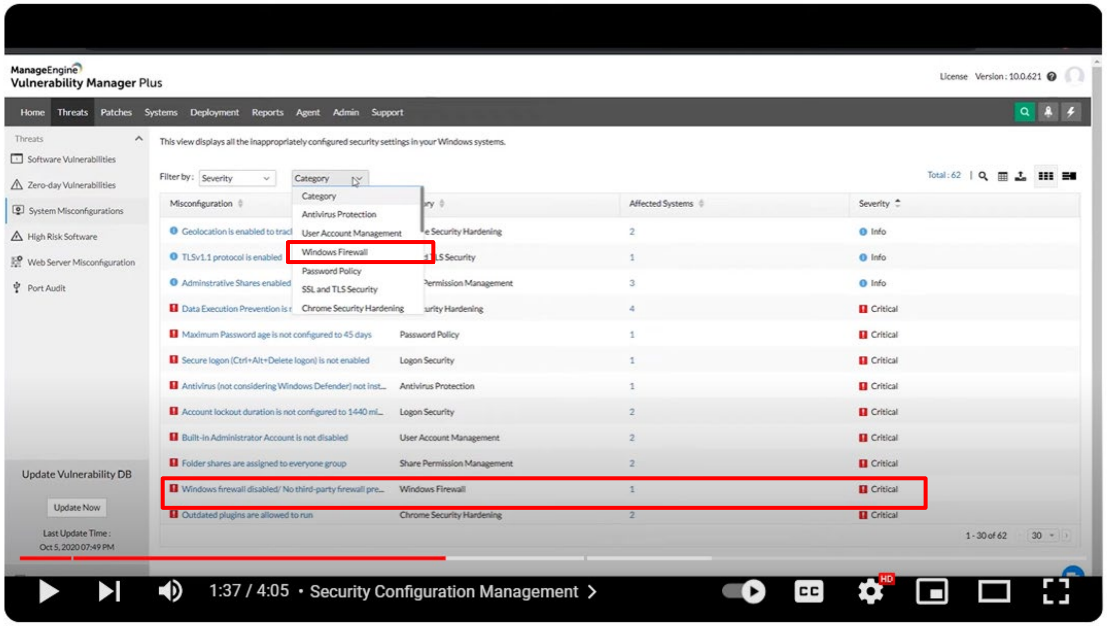
1 - 30 of 62

Security Configuration Management with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=p2Oh87NruMo

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td></td>
<td>


This view displays all the inappropriately configured security settings in your Windows systems.

Last Update Time : Oct 5, 2020 07:49 PM

<table>
<tr><th>Misconfiguration</th><th>ry</th><th>Affected Systems</th><th>Severity</th></tr>
<tr><td>Geolocation is enabled to tracl</td><td>e Security Hardening</td><td>2</td><td>Info</td></tr>
<tr><td>TLSv1.1 protocol is enabled</td><td>LS Security</td><td>1</td><td>Info</td></tr>
<tr><td>Adminstrative Shares enabled</td><td>Permission Management</td><td>3</td><td>Info</td></tr>
<tr><td>Data Execution Prevention is r</td><td>urity Hardening</td><td>4</td><td>Critical</td></tr>
<tr><td>Maximum Password age is not configured to 45 days</td><td>Password Policy</td><td>1</td><td>Critical</td></tr>
<tr><td>Secure logon (Ctrl+Alt+Delete logon) is not enabled</td><td>Logon Security</td><td>1</td><td>Critical</td></tr>
<tr><td>Antivirus (not considering Windows Defender) not inst...</td><td>Antivirus Protection</td><td>1</td><td>Critical</td></tr>
<tr><td>Account lockout duration is not configured to 1440 mi...</td><td>Logon Security</td><td>2</td><td>Critical</td></tr>
<tr><td>Built-in Administrator Account is not disabled</td><td>User Account Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Folder shares are assigned to everyone group</td><td>Share Permission Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Windows firewall disabled/ No third-party firewall pre...</td><td>Windows Firewall</td><td>1</td><td>Critical</td></tr>
<tr><td>Outdated plugins are allowed to run</td><td>Chrome Security Hardening</td><td>2</td><td>Critical</td></tr>
</table>

Security Configuration Management with ManageEngine Vulnerability Manager Plus

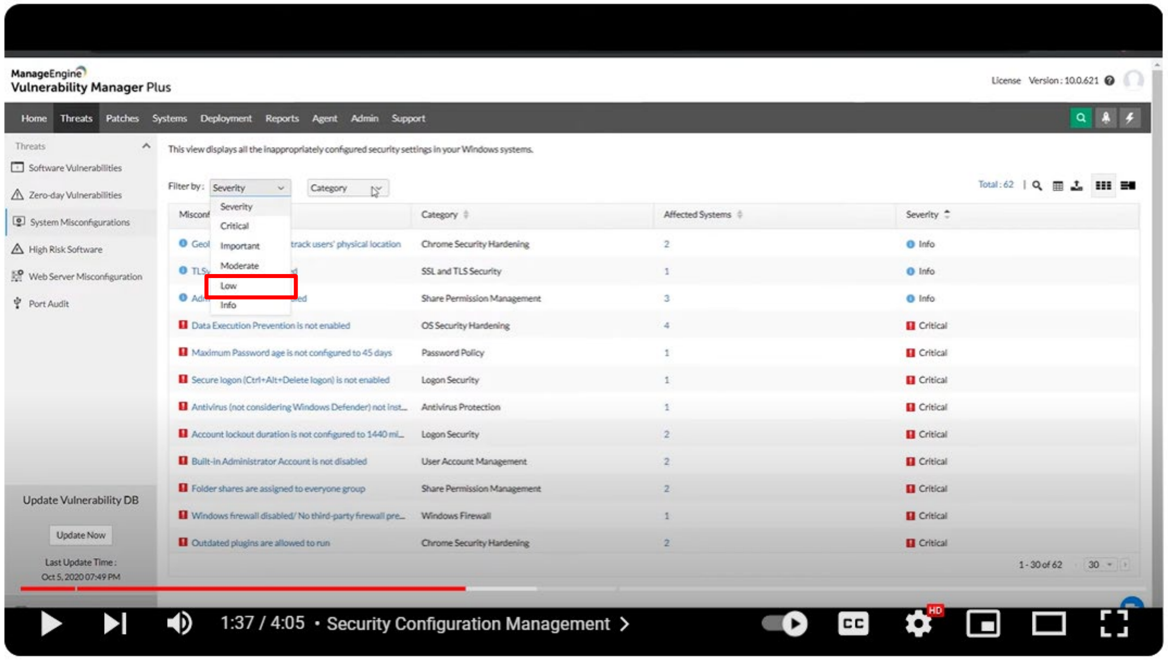
https://www.youtube.com/watch?v=p2Oh87NruMo
</td>
</tr>
<tr>
<td>identifying a sixth event of the plurality of events in connection with the at least one device; and
causing a determination that the at least one of the actual</td>
<td>ManageEngine, when in operation, practices a method of <em>identifying a sixth event of the plurality of events in connection with the at least one device</em> (e.g., any event such as windows firewall related under the firewall category which is not marked as critical) <em>causing a determination that the at least one of the actual vulnerabilities corresponding with the firewall-related information is not susceptible to being taken advantage of by the sixth event identified in connection with the at least one device, utilizing the firewall-related information</em> (e.g., event which is provided category as firewall and the severity level as low indicates</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td>vulnerabilities corresponding with the firewall-related information is not susceptible to being taken advantage of by the sixth event identified in connection with the at least one device, utilizing the firewall-related information; and</td>
<td>that the information is not susceptible to being taken advantage of by the event such as any windows firewall event under the low severity level)

<b>Note:</b> See, for example, the evidence above (where applicable) and below (emphasis added, if any):



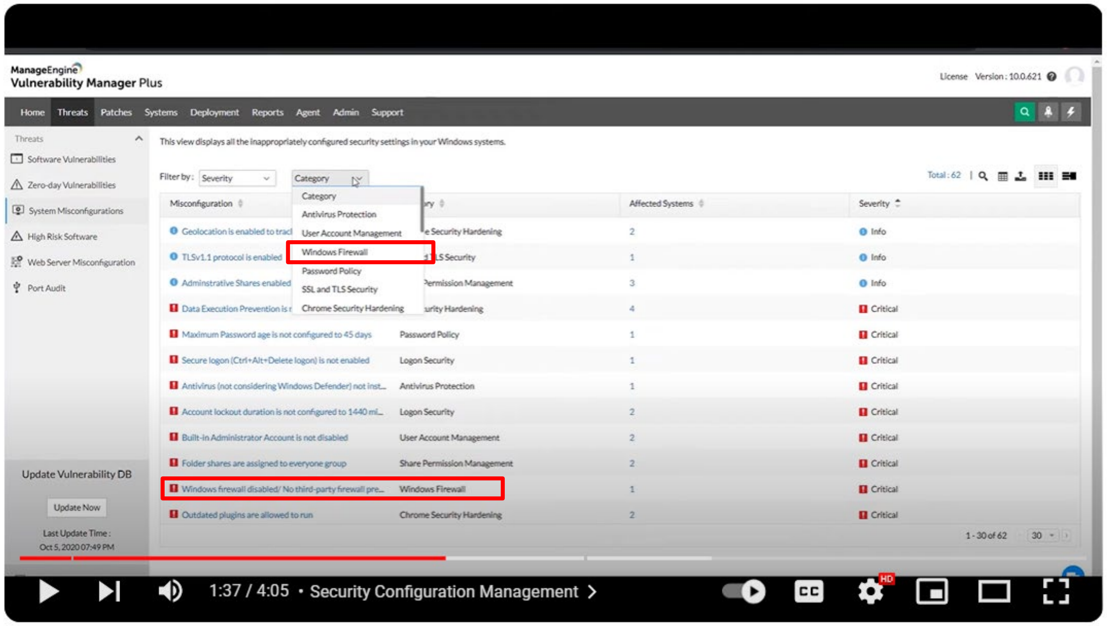
This view displays all the inappropriately configured security settings in your Windows systems.
Last Update Time : Oct 5, 2020 07:49 PM
<table>
<tr><th>Misconf</th><th>Category</th><th>Affected Systems</th><th>Severity</th></tr>
<tr><td>Geol track users' physical location</td><td>Chrome Security Hardening</td><td>2</td><td>Info</td></tr>
<tr><td>TLS d</td><td>SSL and TLS Security</td><td>1</td><td>Info</td></tr>
<tr><td>Adr led</td><td>Share Permission Management</td><td>3</td><td>Info</td></tr>
<tr><td>Data Execution Prevention is not enabled</td><td>OS Security Hardening</td><td>4</td><td>Critical</td></tr>
<tr><td>Maximum Password age is not configured to 45 days</td><td>Password Policy</td><td>1</td><td>Critical</td></tr>
<tr><td>Secure logon (Ctrl+Alt+Delete logon) is not enabled</td><td>Logon Security</td><td>1</td><td>Critical</td></tr>
<tr><td>Antivirus (not considering Windows Defender) not inst...</td><td>Antivirus Protection</td><td>1</td><td>Critical</td></tr>
<tr><td>Account lockout duration is not configured to 1440 mi...</td><td>Logon Security</td><td>2</td><td>Critical</td></tr>
<tr><td>Built-in Administrator Account is not disabled</td><td>User Account Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Folder shares are assigned to everyone group</td><td>Share Permission Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Windows firewall disabled/ No third-party firewall pre...</td><td>Windows Firewall</td><td>1</td><td>Critical</td></tr>
<tr><td>Outdated plugins are allowed to run</td><td>Chrome Security Hardening</td><td>2</td><td>Critical</td></tr>
</table>

<b>Security Configuration Management with ManageEngine Vulnerability Manager Plus</b>

https://www.youtube.com/watch?v=p2Oh87NruMo</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

<table>
<tr>
<td></td>
<td>


Last Update Time : Oct 5, 2020 07:49 PM

This view displays all the inappropriately configured security settings in your Windows systems.

<table>
<tr><th>Misconfiguration</th><th>ry</th><th>Affected Systems</th><th>Severity</th></tr>
<tr><td>Geolocation is enabled to tracl</td><td>e Security Hardening</td><td>2</td><td>Info</td></tr>
<tr><td>TLSv1.1 protocol is enabled</td><td>LS Security</td><td>1</td><td>Info</td></tr>
<tr><td>Adminstrative Shares enabled</td><td>ermission Management</td><td>3</td><td>Info</td></tr>
<tr><td>Data Execution Prevention is r</td><td>urity Hardening</td><td>4</td><td>Critical</td></tr>
<tr><td>Maximum Password age is not configured to 45 days</td><td>Password Policy</td><td>1</td><td>Critical</td></tr>
<tr><td>Secure logon (Ctrl+Alt+Delete logon) is not enabled</td><td>Logon Security</td><td>1</td><td>Critical</td></tr>
<tr><td>Antivirus (not considering Windows Defender) not inst...</td><td>Antivirus Protection</td><td>1</td><td>Critical</td></tr>
<tr><td>Account lockout duration is not configured to 1440 mi...</td><td>Logon Security</td><td>2</td><td>Critical</td></tr>
<tr><td>Built-in Administrator Account is not disabled</td><td>User Account Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Folder shares are assigned to everyone group</td><td>Share Permission Management</td><td>2</td><td>Critical</td></tr>
<tr><td>Windows firewall disabled/ No third-party firewall pre...</td><td>Windows Firewall</td><td>1</td><td>Critical</td></tr>
<tr><td>Outdated plugins are allowed to run</td><td>Chrome Security Hardening</td><td>2</td><td>Critical</td></tr>
</table>

Security Configuration Management with ManageEngine Vulnerability Manager Plus

https://www.youtube.com/watch?v=p2Oh87NruMo
</td>
</tr>
<tr>
<td>at at least one administrator computer:
in response to administrator action, causing setting, before the first and second events, of a first policy associated with utilizing the</td>
<td>ManageEngine, when in operation, practices a method wherein <i>at least one administrator computer</i> (e.g., admin role or technician role defined user has a computer) <i>in response to administrator action</i> (e.g., admin defined or technician defined rules), <i>causing setting, before the first and second events, of a first policy associated with utilizing the data inspection-related information that is applied to a group including each of the plurality of devices that has the at least one operating system;</i> (e.g., can define, deploy, re-deploy tasks, patches, configurations and scan operations)
<b>Note:</b> See, for example, the evidence above (where applicable) and below (emphasis added, if any):</td>
</tr>
</table>

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

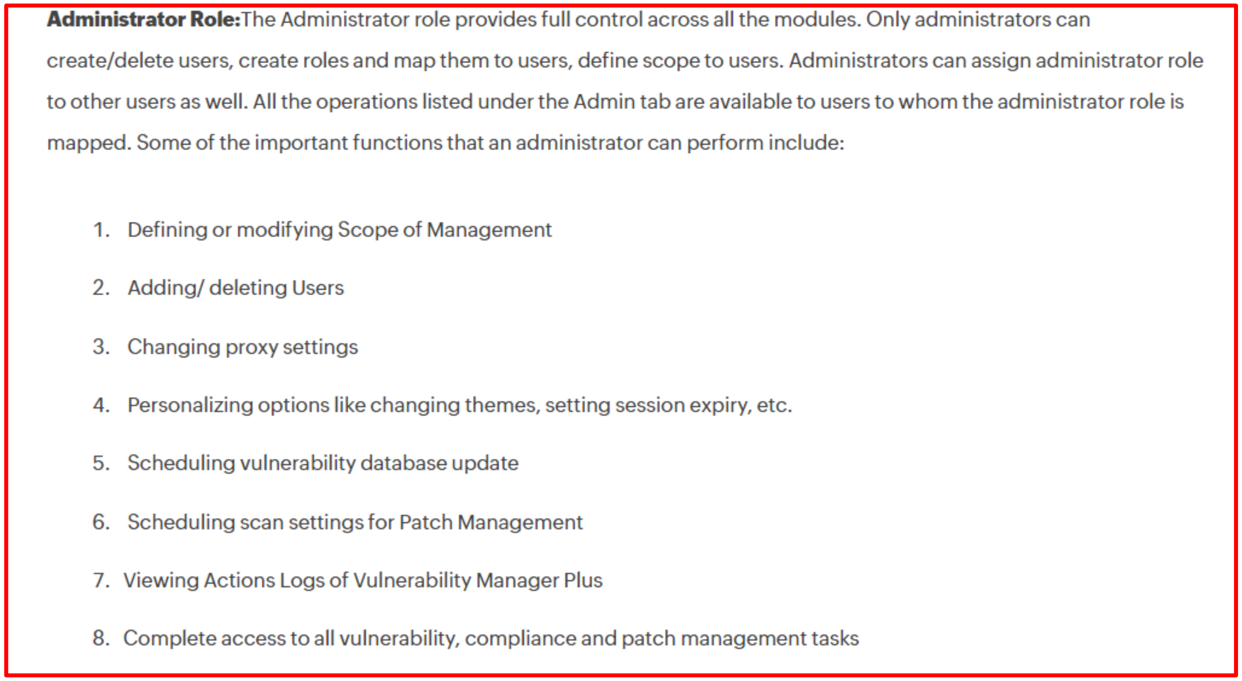
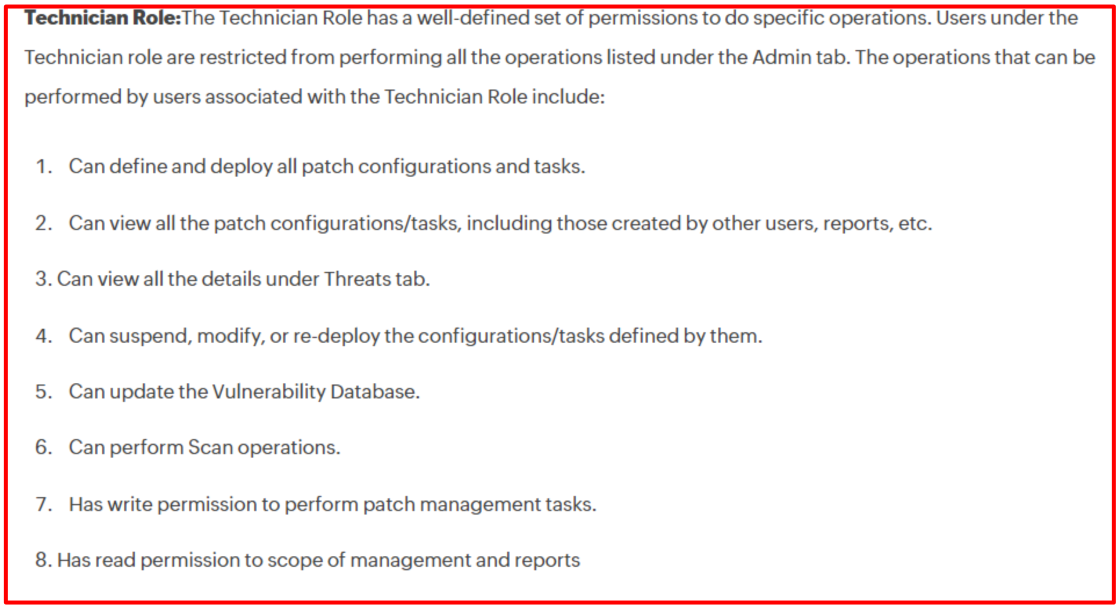
data inspection-related information that is applied to a group including each of the plurality of devices that has the at least one operating system;	 **Administrator Role:**The Administrator role provides full control across all the modules. Only administrators can create/delete users, create roles and map them to users, define scope to users. Administrators can assign administrator role to other users as well. All the operations listed under the Admin tab are available to users to whom the administrator role is mapped. Some of the important functions that an administrator can perform include: 1. Defining or modifying Scope of Management 2. Adding/ deleting Users 3. Changing proxy settings 4. Personalizing options like changing themes, setting session expiry, etc. 5. Scheduling vulnerability database update 6. Scheduling scan settings for Patch Management 7. Viewing Actions Logs of Vulnerability Manager Plus 8. Complete access to all vulnerability, compliance and patch management tasks https://www.manageengine.com/vulnerability-management/help/user-administration.html

EXHIBIT 10

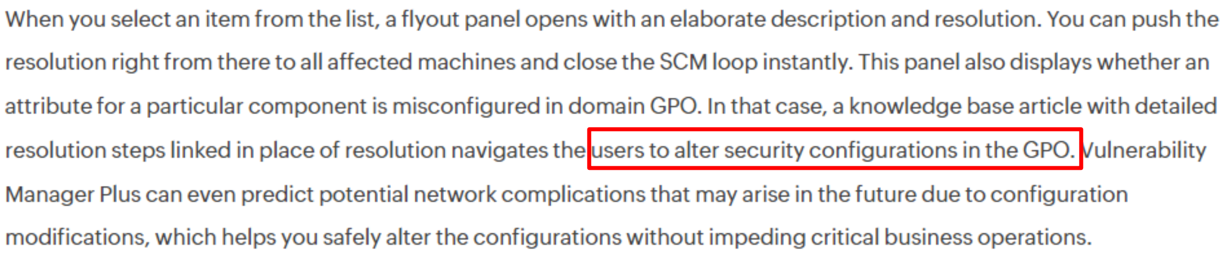
U.S. Patent No 10,873,595 v. Zoho



Technician Role: The Technician Role has a well-defined set of permissions to do specific operations. Users under the Technician role are restricted from performing all the operations listed under the Admin tab. The operations that can be performed by users associated with the Technician Role include:

1. Can define and deploy all patch configurations and tasks.
2. Can view all the patch configurations/tasks, including those created by other users, reports, etc.
3. Can view all the details under Threats tab.
4. Can suspend, modify, or re-deploy the configurations/tasks defined by them.
5. Can update the Vulnerability Database.
6. Can perform Scan operations.
7. Has write permission to perform patch management tasks.
8. Has read permission to scope of management and reports

https://www.manageengine.com/vulnerability-management/help/user-administration.html



When you select an item from the list, a flyout panel opens with an elaborate description and resolution. You can push the resolution right from there to all affected machines and close the SCM loop instantly. This panel also displays whether an attribute for a particular component is misconfigured in domain GPO. In that case, a knowledge base article with detailed resolution steps linked in place of resolution navigates the users to alter security configurations in the GPO. Vulnerability Manager Plus can even predict potential network complications that may arise in the future due to configuration modifications, which helps you safely alter the configurations without impeding critical business operations.

https://www.manageengine.com/vulnerability-management/security-configuration-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

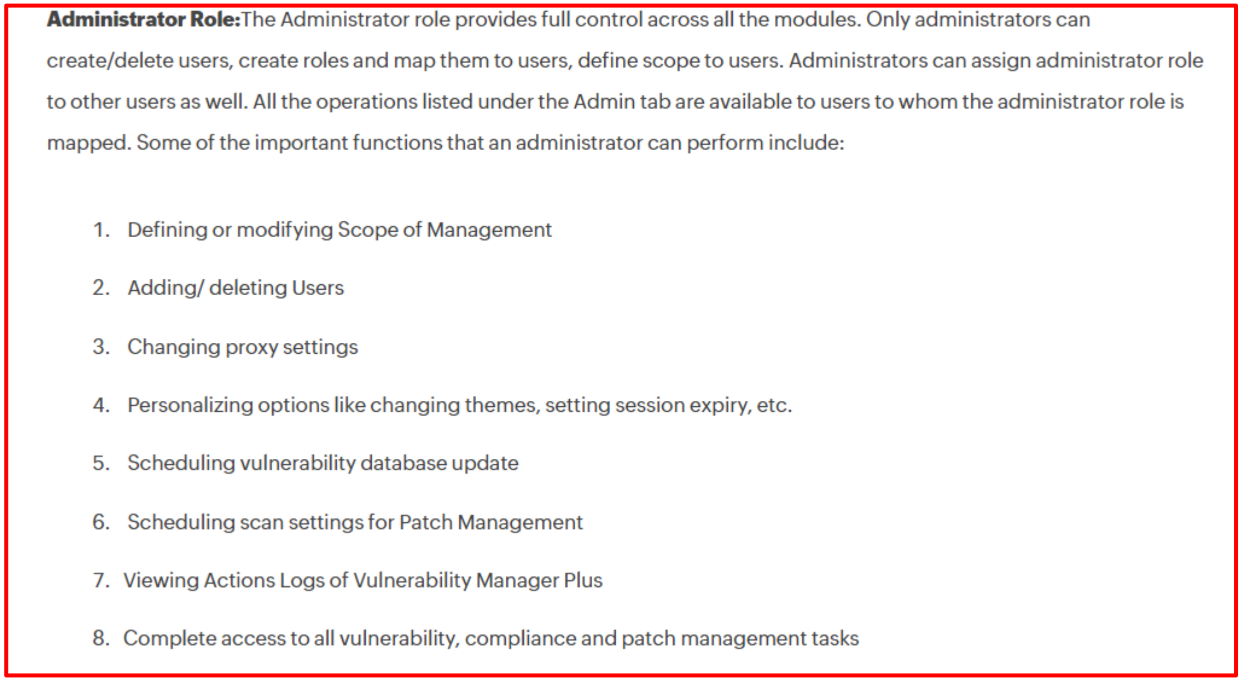
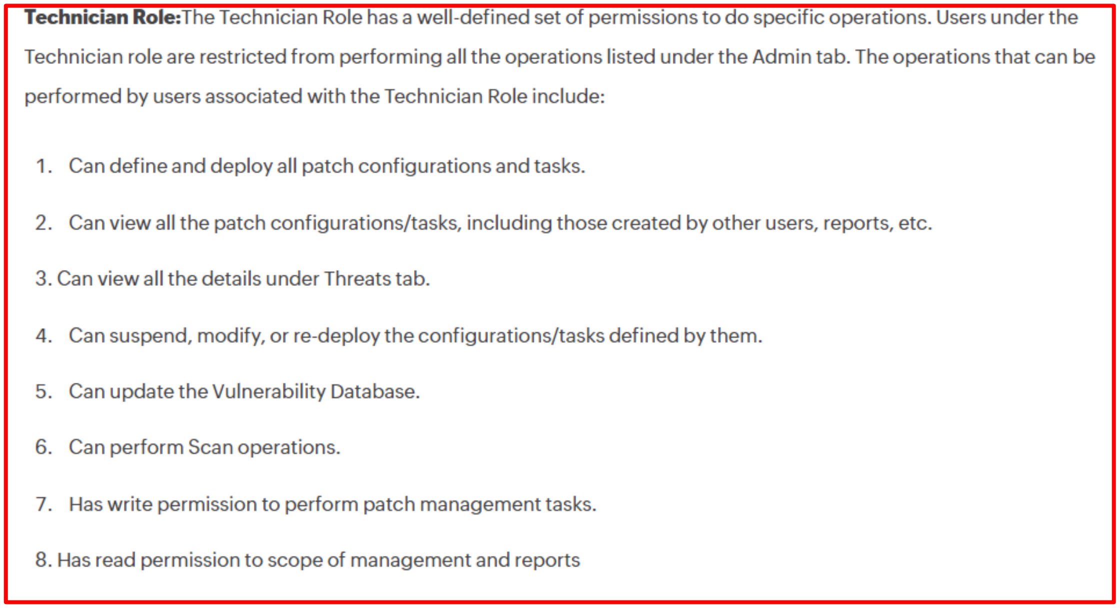
in response to administrator action, causing setting, before the third and fourth events, of a second policy associated with utilizing the traffic inspection-related information that is applied the group including each of the plurality of devices that has the at least one operating system; and	ManageEngine, when in operation, practices a method wherein *in response to administrator action* (e.g., admin defined or technician defined rules), *causing setting, before the third and fourth events, of a second policy associated with utilizing the traffic inspection-related information that is applied the group including each of the plurality of devices that has the at least one operating system* (e.g., can define, deploy, re-deploy tasks, patches, configurations and scan operations) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  **Administrator Role:**The Administrator role provides full control across all the modules. Only administrators can create/delete users, create roles and map them to users, define scope to users. Administrators can assign administrator role to other users as well. All the operations listed under the Admin tab are available to users to whom the administrator role is mapped. Some of the important functions that an administrator can perform include: 1. Defining or modifying Scope of Management 2. Adding/ deleting Users 3. Changing proxy settings 4. Personalizing options like changing themes, setting session expiry, etc. 5. Scheduling vulnerability database update 6. Scheduling scan settings for Patch Management 7. Viewing Actions Logs of Vulnerability Manager Plus 8. Complete access to all vulnerability, compliance and patch management tasks

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

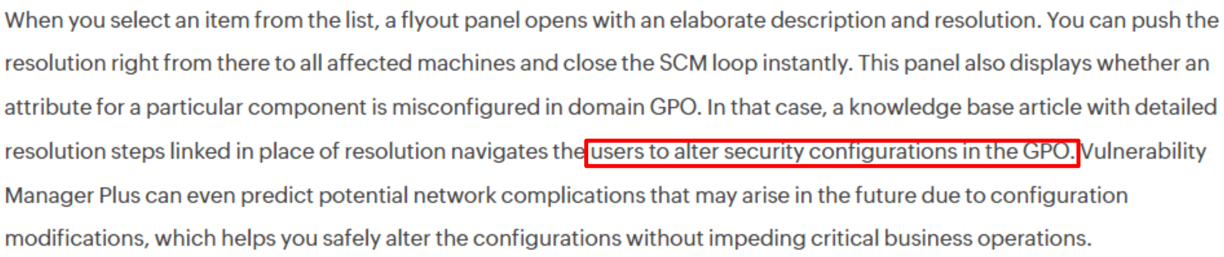
https://www.manageengine.com/vulnerability-management/help/user-administration.html



Technician Role: The Technician Role has a well-defined set of permissions to do specific operations. Users under the Technician role are restricted from performing all the operations listed under the Admin tab. The operations that can be performed by users associated with the Technician Role include:

1. Can define and deploy all patch configurations and tasks.
2. Can view all the patch configurations/tasks, including those created by other users, reports, etc.
3. Can view all the details under Threats tab.
4. Can suspend, modify, or re-deploy the configurations/tasks defined by them.
5. Can update the Vulnerability Database.
6. Can perform Scan operations.
7. Has write permission to perform patch management tasks.
8. Has read permission to scope of management and reports

https://www.manageengine.com/vulnerability-management/help/user-administration.html



When you select an item from the list, a flyout panel opens with an elaborate description and resolution. You can push the resolution right from there to all affected machines and close the SCM loop instantly. This panel also displays whether an attribute for a particular component is misconfigured in domain GPO. In that case, a knowledge base article with detailed resolution steps linked in place of resolution navigates the users to alter security configurations in the GPO. Vulnerability Manager Plus can even predict potential network complications that may arise in the future due to configuration modifications, which helps you safely alter the configurations without impeding critical business operations.

https://www.manageengine.com/vulnerability-management/security-configuration-management.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

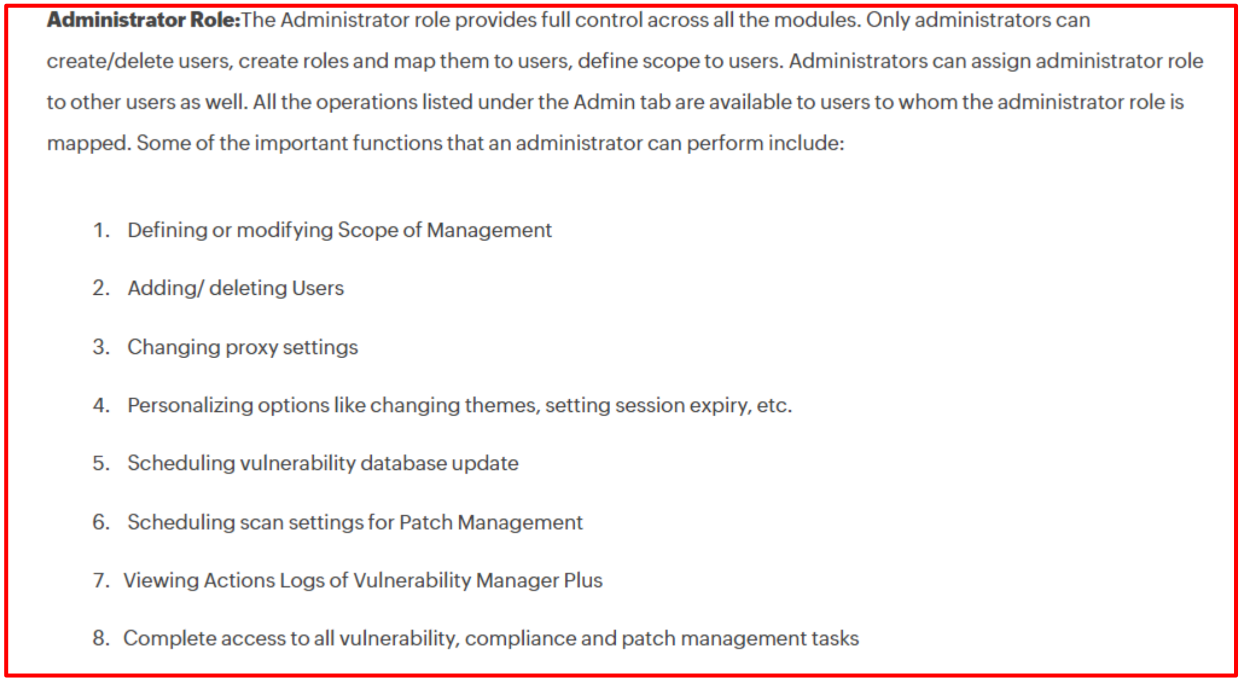
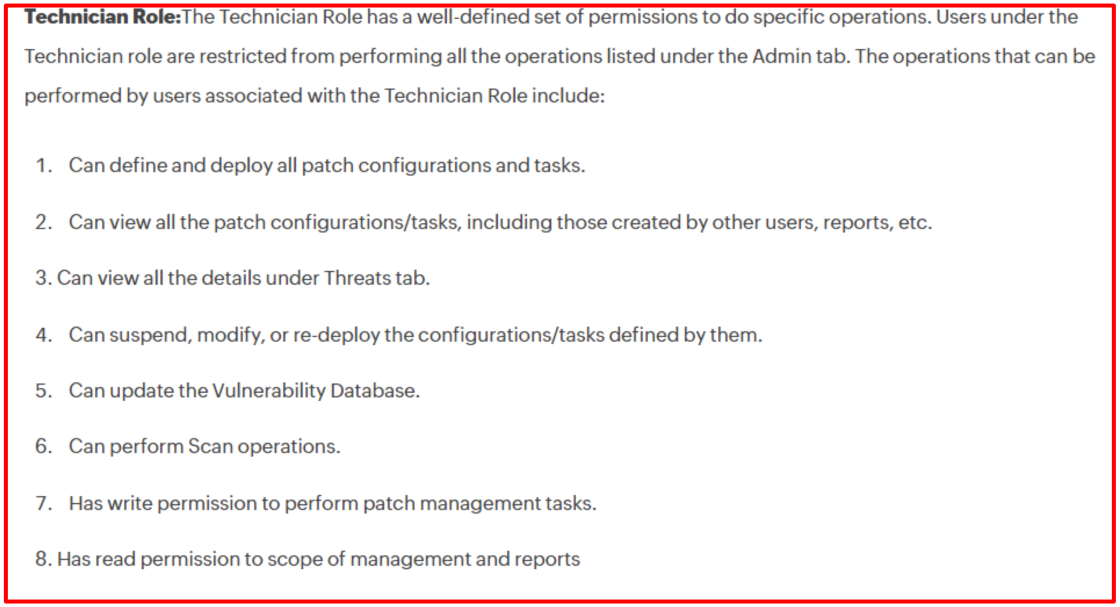
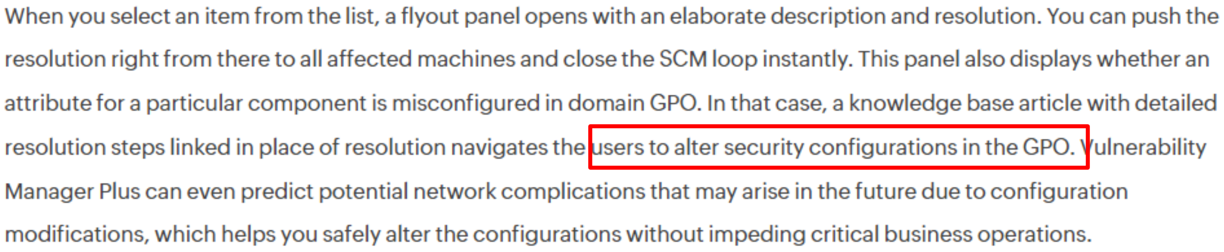
in response to administrator action, causing setting, before the fifth and sixth events, of a third policy associated with utilizing the firewall-related information that is applied to the group including each of the plurality of devices that has the at least one operating system.	ManageEngine, when in operation, practices a method wherein *in response to administrator action* (e.g., admin defined or technician defines rules)*, causing setting, before the fifth and sixth events of a third policy associated with utilizing the firewall-related information that is applied to the group including each of the plurality of devices that has the at least one operating system.* (e.g., can define, deploy, re-deploy tasks, patches, configurations and scan operations) **Note:** See, for example, the evidence above (where applicable) and below (emphasis added, if any):  **Administrator Role:**The Administrator role provides full control across all the modules. Only administrators can create/delete users, create roles and map them to users, define scope to users. Administrators can assign administrator role to other users as well. All the operations listed under the Admin tab are available to users to whom the administrator role is mapped. Some of the important functions that an administrator can perform include: 1. Defining or modifying Scope of Management 2. Adding/ deleting Users 3. Changing proxy settings 4. Personalizing options like changing themes, setting session expiry, etc. 5. Scheduling vulnerability database update 6. Scheduling scan settings for Patch Management 7. Viewing Actions Logs of Vulnerability Manager Plus 8. Complete access to all vulnerability, compliance and patch management tasks https://www.manageengine.com/vulnerability-management/help/user-administration.html

EXHIBIT 10

U.S. Patent No 10,873,595 v. Zoho

	 **Technician Role:**The Technician Role has a well-defined set of permissions to do specific operations. Users under the Technician role are restricted from performing all the operations listed under the Admin tab. The operations that can be performed by users associated with the Technician Role include: 1. Can define and deploy all patch configurations and tasks. 2. Can view all the patch configurations/tasks, including those created by other users, reports, etc. 3. Can view all the details under Threats tab. 4. Can suspend, modify, or re-deploy the configurations/tasks defined by them. 5. Can update the Vulnerability Database. 6. Can perform Scan operations. 7. Has write permission to perform patch management tasks. 8. Has read permission to scope of management and reports https://www.manageengine.com/vulnerability-management/help/user-administration.html  When you select an item from the list, a flyout panel opens with an elaborate description and resolution. You can push the resolution right from there to all affected machines and close the SCM loop instantly. This panel also displays whether an attribute for a particular component is misconfigured in domain GPO. In that case, a knowledge base article with detailed resolution steps linked in place of resolution navigates the users to alter security configurations in the GPO. Vulnerability Manager Plus can even predict potential network complications that may arise in the future due to configuration modifications, which helps you safely alter the configurations without impeding critical business operations. https://www.manageengine.com/vulnerability-management/security-configuration-management.html